COMODO
Creating Trust Online®

Comodo
Endpoint Security Manager
Software Version 1.6

CIS Configuration Editor Guide
Guide Version 1.6.010511

Comodo Security Solutions
1255 Broad Street
STE 100
Clifton, NJ 07013

Table of Contents

1. Introduction to Comodo Internet Security Configuration Editor

Overview

After installation of Comodo Internet Security (CIS) on endpoint computers, administrators **must** deploy a CIS configuration to activate the software. There are two ways in which this can be done:

Deploy a preconfigured configuration

This is the default and recommended option and allows admins to quickly implement a Comodo preset configuration according to requirements.

Click here for a brief explanation of how to roll out a preset configuration.

OR

Create a custom configuration using the built in CIS Configuration Editor

This option involves the administrator using the built in CIS Configuration Editor to specify custom settings.

Click Here to learn how to use the editor and roll out a custom configuration

Prerequisites to deploying a CIS configuration

There are some prerequisites that are required to be implemented prior to deploying any configuration for the application to run effectively. The following steps should already have been completed before configuring and deploying a custom or predefined configuration:

- **Import the Network and Choose Which Computers to Manage**
- **Install the Remote Agent**
- **Upload Installation Package**
- **Install CIS on target machines**

If the steps above have already been completed then proceed directly to '**Deploy a Preset Configuration**' or '**Deploy a Custom Configuration**'.

2. Prerequisites to Deploying a CIS Configuration

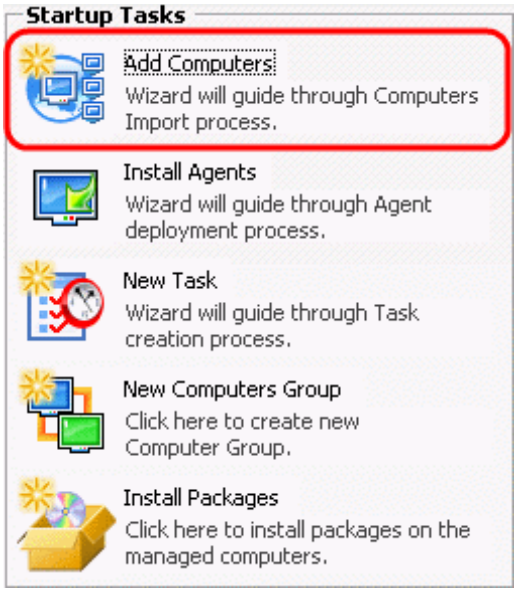
Step 1: Import the Network and Choose Which Computers to Manage

To control any computer or network, first import it into the CESM console. Next, designate 'Managed' computers and install the

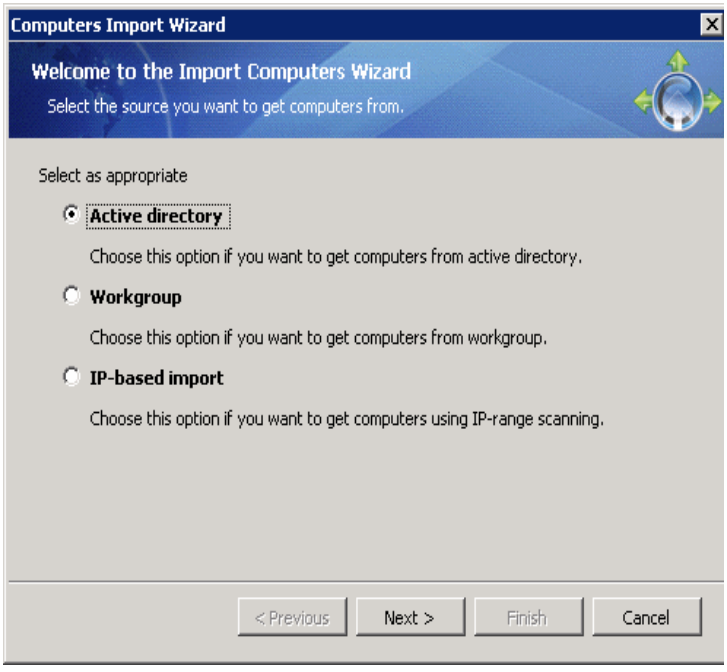
CESM Remote Agent on them.

To start importing the computers:

1. Open Start Page (Click 'View > Start Page' if it is not already visible). Click the 'Add Computers' link to initiate the import computers wizard.

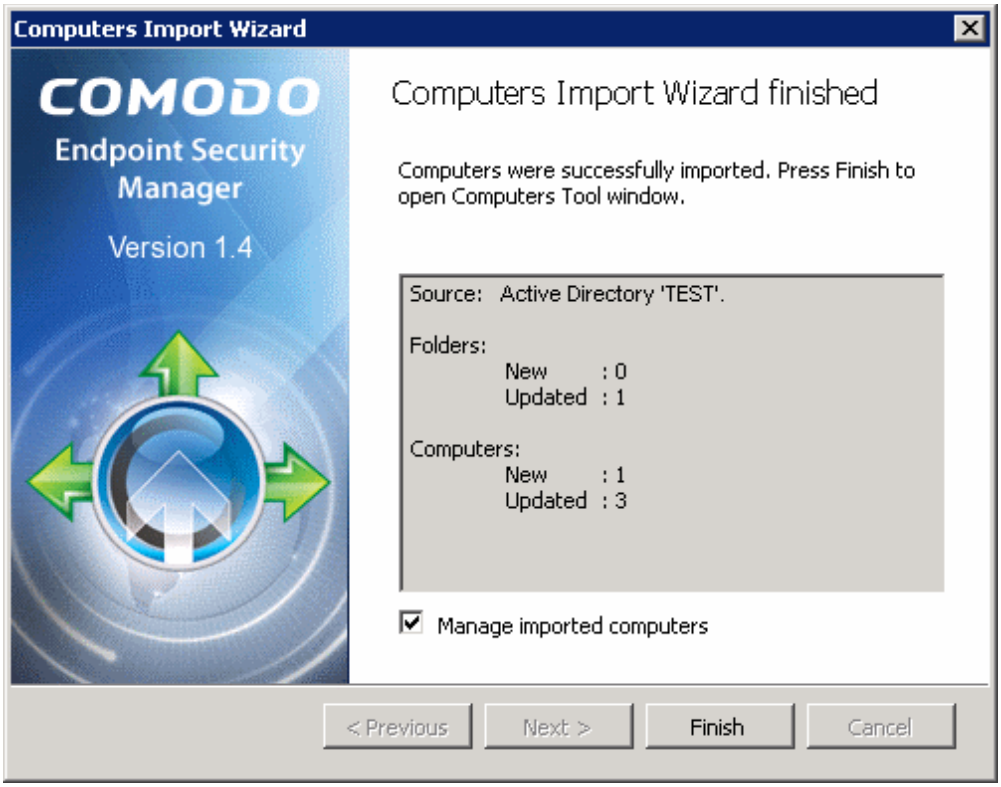


2. Choose import from Active Directory, Workgroup or by IP address and click 'Next'.



- **Active Directory** - Either Import from the current domain or manually specify another domain. Leave 'Use Advanced Import Settings' enabled to filter the type of computers that are imported
- **Workgroup** - Select from the list of detected Workgroups
- **IP Address** - Manually specify the IP or range of IP addresses / DNS Names

3. Click 'Next' to begin the import. CESM detects and automatically import computers according to the administrator preferences. The results are displayed as the final step of the wizard.



Note: Leaving the 'Manage imported computers' checkbox enabled automatically assigns 'Managed' status to ALL imported computers. A computer needs to be 'Managed' in order to install the Remote Agent on it. A 'Managed' computer is colored blue and automatically uses one of the licenses. Alternatively, it may be disabled and 'Managed' status can be assigned later by right clicking on specific computers.

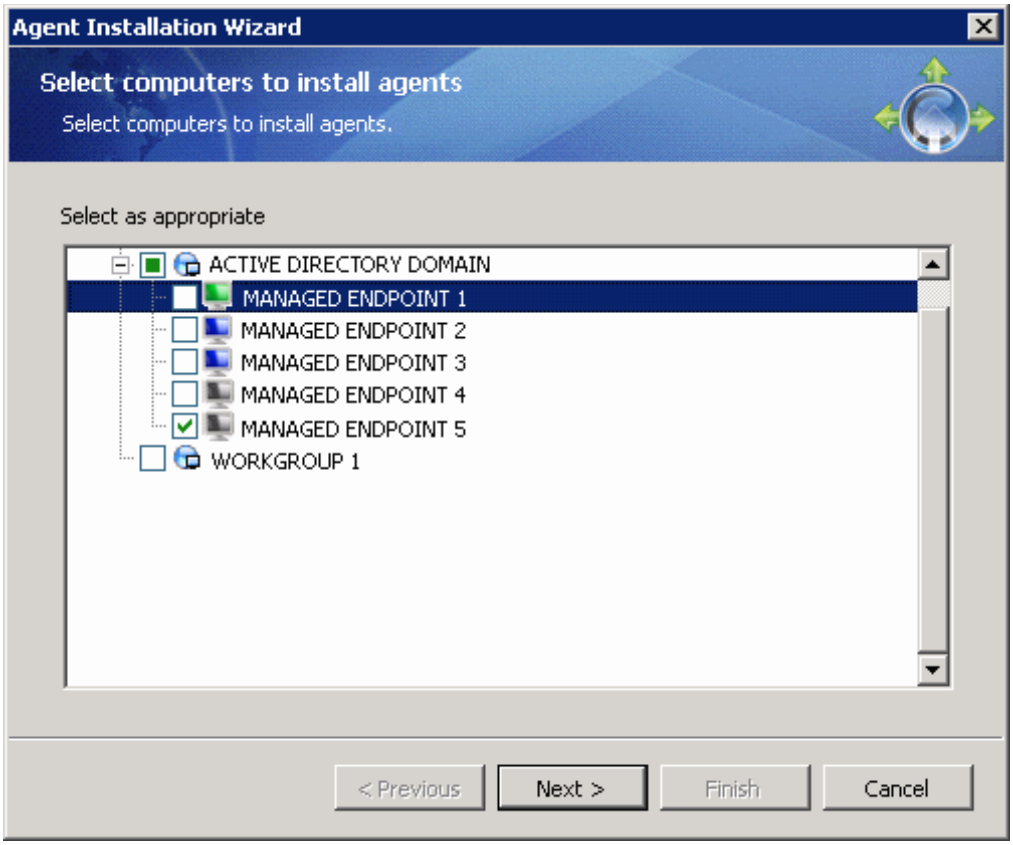
Step 2: Install the Remote Agent

The next step is to install the Remote Agent on the Managed Computers. This allows the endpoint to communicate with CESM central service and the Administrative console.

To install the Remote Agent:

1.Click 'Install Agents' link in the 'Start Page'.

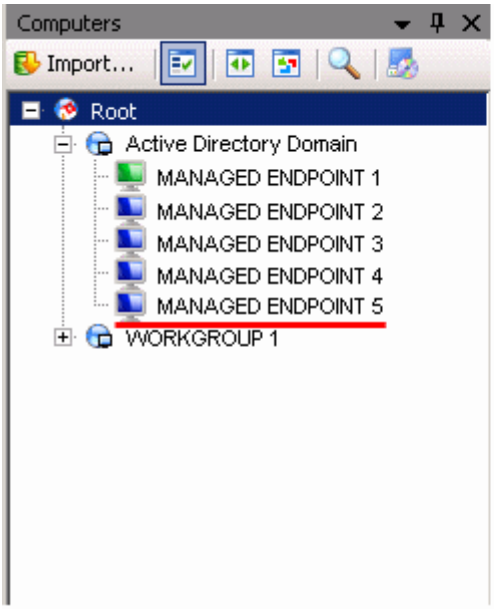
2. Select the Managed computers in which the remote agent is to be installed. Select all computers in a domain or Workgroup by selecting the checkbox next to the domain or Workgroup name. Click 'Next'.



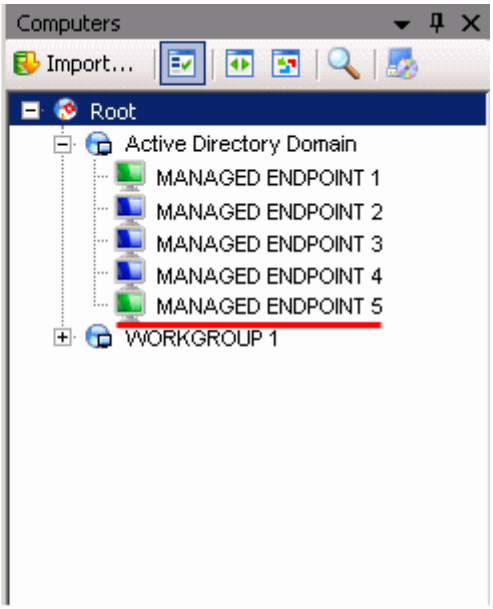
4. To install the Agent on the endpoints, enter the User Name and Password of a local administrator. If you imported the workstation(s) from Active Directory then you can use the AD administrator user-name and password instead. Click 'Next' to continue.
5. The wizard runs a diagnostics check to make sure there are no problems that prevents the installation. If problems are discovered then a message stating the nature of the problem is displayed to take corrective actions. If no problems are detected then a 'Ready to Install' status message is displayed.
6. Select the computers in which the Agent is to be installed then click 'Next'. Finally, click 'Install'.
7. After installation, the Agent attempts to connect to the Central Service. If the connection attempt is successful then the color of the icon representing those machines changes from Blue (Managed but not connected to Central Service) to Green(Managed and successfully connected to CESM Central Service). The 'Computers' window in the CESM console displays the imported computers of the network with icon colors indicating their status as shown below:

Icon Image	Status
	Unmanaged Computers
	Managed but not connected to CESM Central Service. CESM remote agent must be installed.
	Managed and connected to CESM Central Service.
	Managed, connected to CESM Central Service *and* CESM Warranty is enabled.

In the example below, the machine color of MANAGED ENDPOINT 5 had changed from blue to Green after it is successfully connected to CESM Central Service.



Managed but Agent not installed



Managed. Agent installed and connected

Then Comodo security products can be installed and tasks can be deployed on them.

Step 3: Upload Installation Package

CESM 'Packages' are installer files for Comodo security applications such as CIS and CDE and come in the form of .msi files. First upload the appropriate Package to CESM for installing the application to the required endpoints remotely.

To upload an installation package:

1. Right click on a managed computer in the computers window, point to 'Control' and select 'Install Agent' from the context sensitive menu or click 'New Installation Package' link in the 'Start Page'.
2. Type a name (mandatory) and a description (optional) for the new package in the respective fields in the 'New Package' dialog.
3. To specify the package to be uploaded, click the ellipsis button beside the 'File:' text box, browse to the local or network location which contain comodo.msi files and select the package file. The selected file is displayed with the path in the 'File:' text field.
4. Click 'Save' to complete the process.

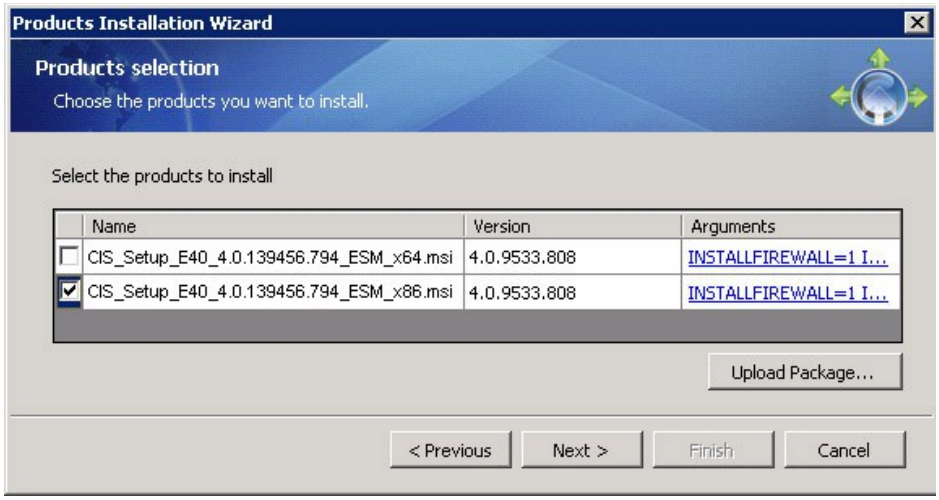
The package file is now uploaded and ready for installation to the endpoints.

Step 4: Install CIS on Target Machines

Next, to install CIS on to the endpoints, create a task containing sequence of actions to be executed on the managed computers using the 'Products Installation Wizard'.

1. Start the wizard by clicking 'Install Packages' on the Start page
2. Type a name (mandatory) and a description (optional) for the new task in the 'Task Properties' dialog and click 'Next'.
3. Select to execute the new task on to individual computers or a group of computers and then select the computers or groups from the displayed computer tree.
4. Remove incompatible products. Before commencing the installation of Comodo packages, the wizard will first check for any incompatible products and offer to uninstall them for you. This includes items such as third party antivirus/firewall products. CESM may need to reboot the endpoint machine(s) to complete the uninstall process. The user of the remote endpoint will be notified of this with a pop-up message on their desktop. They will be offered the opportunity to postpone the reboot for 10 minutes or initiate the reboot immediately. If the user takes no action then their machine will automatically reboot after a 3 minute count-down.

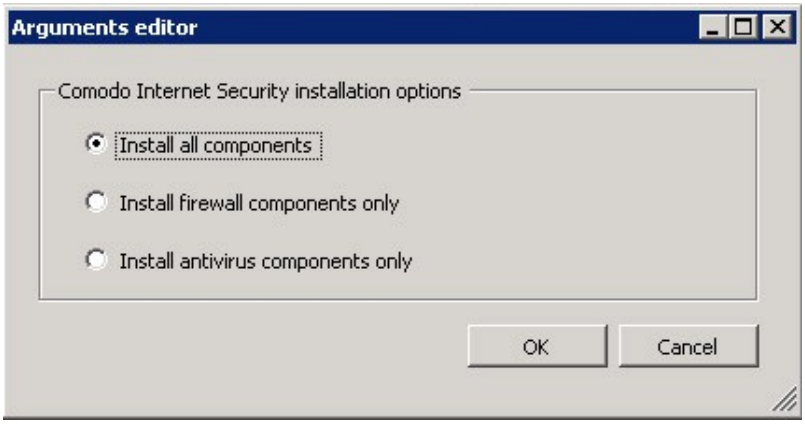
5. Check if newer software is available. The wizard now offers to contact Comodo servers to check whether the packages that have been uploaded to the CESM Console are the latest versions. Click 'Check for updates' to do this.



If newer packages are discovered you should click the 'Update' button to download the latest versions. Click 'Next' to continue.

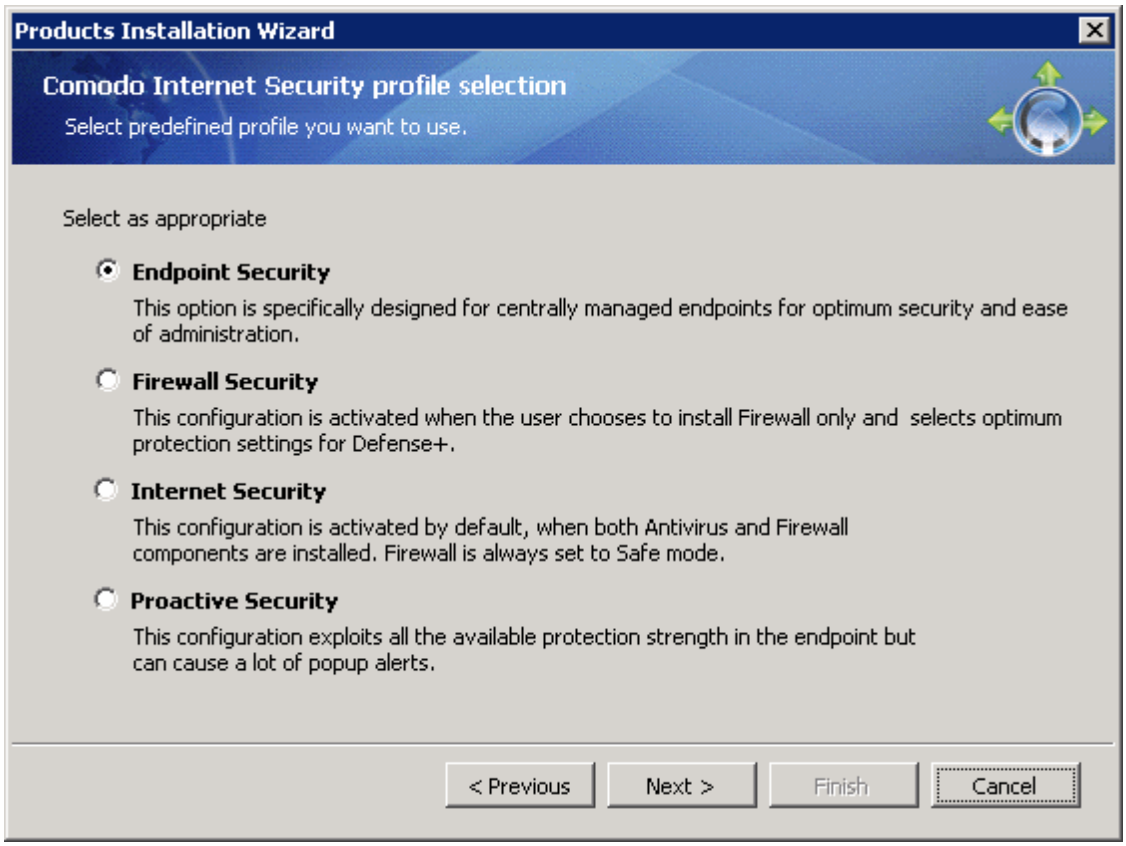
6. Select packages and configure installation options. The next part of the wizard allows you to choose which products to install and to specify installation preferences:

- CESM 'Packages' are the installer files for Comodo security applications such as CIS and CDE and come in the form of .msi files. The names and version numbers of packages that are available for installation are clearly listed. In the example above we have chosen to install the 32 bit version of CIS (filename ends with '_x86.msi). If you wish to install on 64 bit Windows systems then choose filenames ending in 'x64.msi').
- At this point, you also have the opportunity to upload additional packages by clicking 'Upload Package...'. Any new packages you add will be immediately uploaded and added to the list.
- To modify CIS installation options click on the blue underlined text in the 'Arguments' column. You can choose to install all components (both firewall and AV) or just the firewall or antivirus components. The default is to 'Install all components'.



If you chose to install 'All Components' then you next need to select a security profile for CIS:

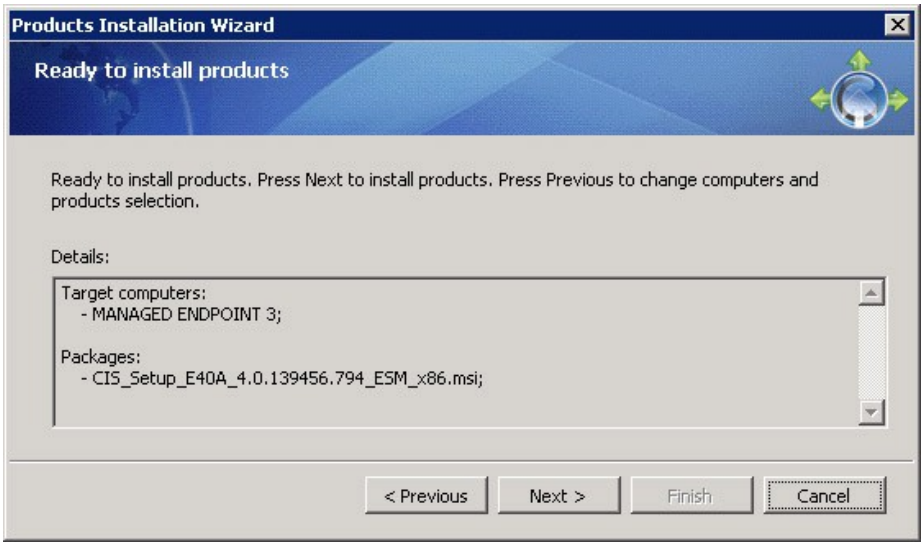
A CIS 'Profile' is predefined security configuration designed for a range of deployment scenarios. 'Endpoint Security' is the default profile and has been specifically designed for centrally managed endpoints. It delivers a great marriage of security and ease of administration is recommended for most networks. 'Proactive Security' turns all security settings to their highest levels but Administrators may experience a trade-off in the higher number of alerts/requests that are generated.



Background Note: Even after deployment, each of these presets can be re-configured by the Administrator according to their specific needs. For more details on CIS configurations, refer to the section 'The Sequence Manager Window > Table of Actions' in the CESM Administrator Guide.

Once you have chosen your profile, click 'Next' to continue.

7. Finalization. The last part of the wizard is simply to review and confirm your installation options then initiate the installation process:



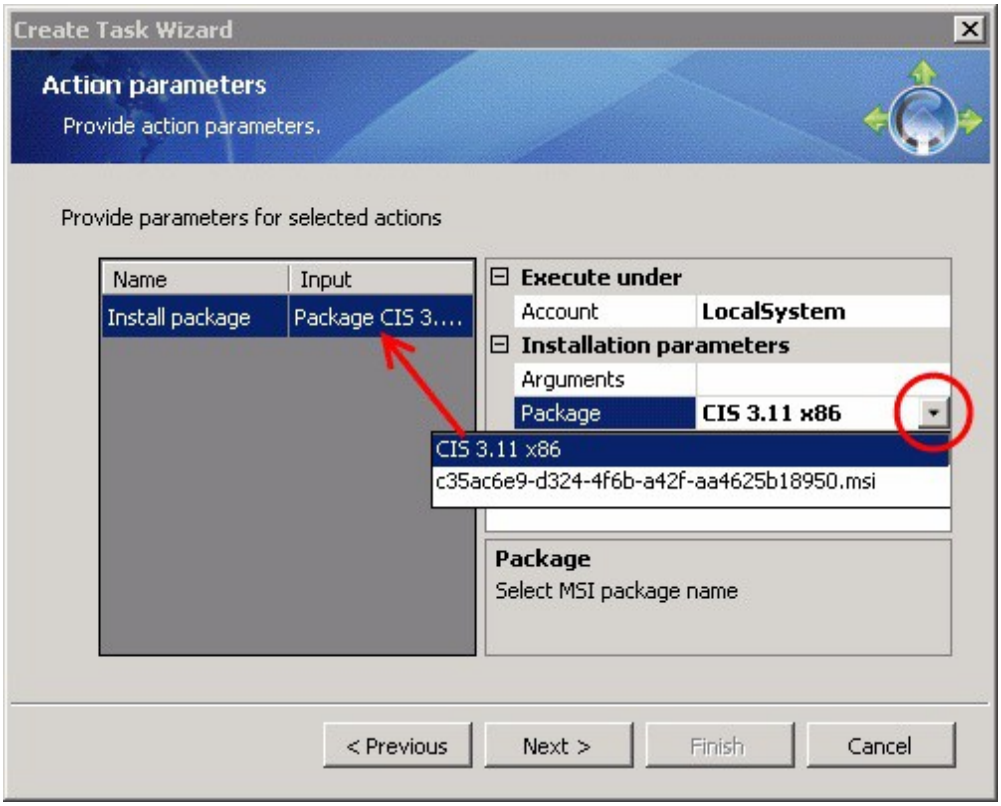
If you wish, you can click 'Previous' to go back and change any settings. Clicking 'Next' will install CIS on your target endpoint machines.

Note: The process outlined above is the easiest, but not the only way, to install CIS.

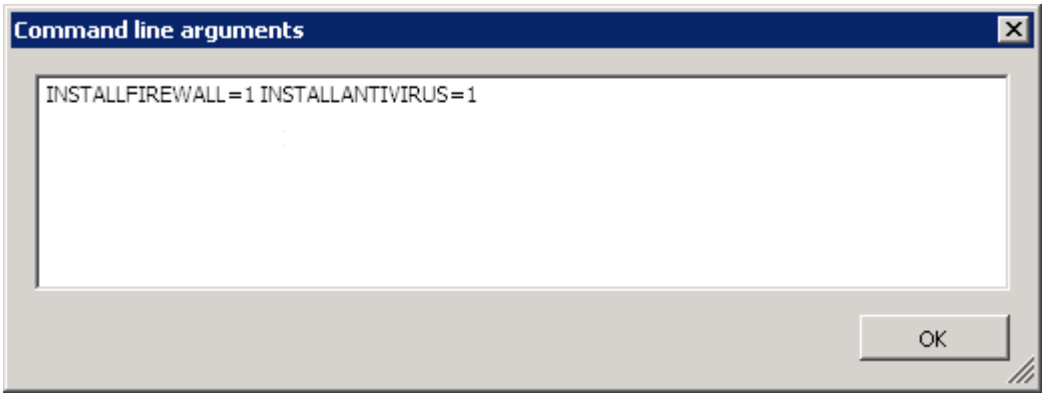
Administrators can also install CIS by right-clicking on target machines and selecting 'Install' or by manually creating a new Task. Please refer to the full administrator's guide if you would like to know more about these alternatives.

Note on 'partial' installation options for Comodo Internet Security

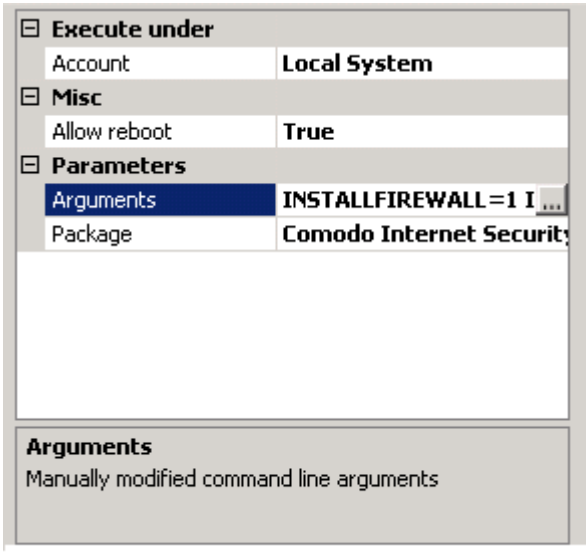
Administrators have the option to install *only* the firewall or *only* the antivirus components of Comodo Internet Security (CIS). This is done by typing a small command into the 'Arguments' field in the 'Installation Parameters' pane whilst configuring a Sequence with the 'Install Package' Action with CIS as the package to be installed.



To effect one of the options above, the administrator has to enter a command into the 'Arguments' field. The command can be entered by clicking the ellipsis ... button on the right end of the Arguments Field and typing the command in the Command Line Arguments text dialog:



- To Install Firewall and Defense+ BUT NOT Antivirus type the following in the command line arguments: **INSTALLFIREWALL=1 INSTALLANTIVIRUS=0**

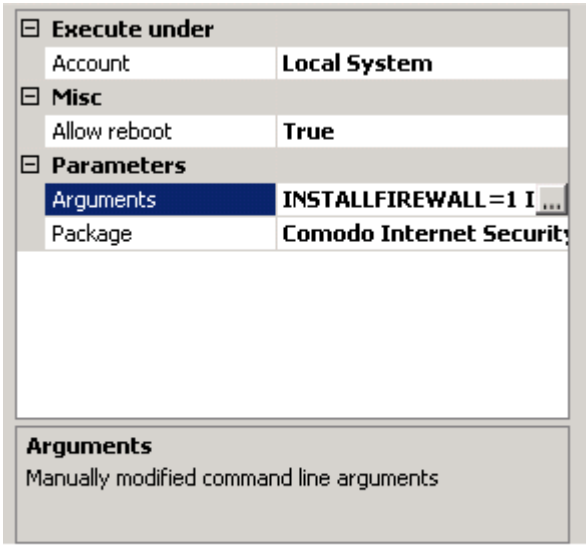


Install Firewall and Defense+ Only

The command is displayed in the Arguments fields.

- To Install the **full CIS suite** (Antivirus, Firewall and Defense+), type the following in the command line arguments:

INSTALLFIREWALL=1 INSTALLANTIVIRUS=1



Install Complete Suite (Antivirus, Firewall and Defense+)

The command is displayed in the Arguments fields.

- To install the full Antivirus only, simply **leave the argument field empty** (do not type anything - this is the default setting).

3. Deploy Preset Configuration

CIS ships with five Predefined Configurations containing preset security settings and also allows Administrators to manually define their own custom configurations.

Note 1: For more details on CIS Preset configurations refer to 'The Sequence Manager Window > Table of Actions' section in the main CESM Administrator Guide.

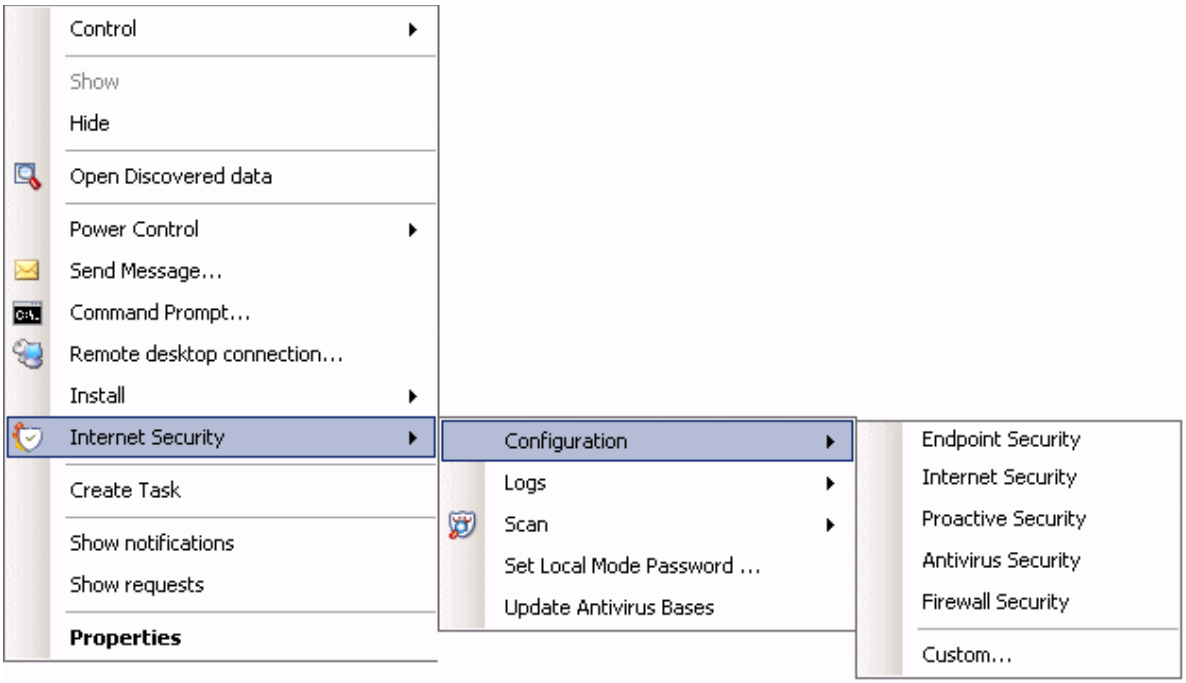
Note 2: For more details on CIS Manual Configuration refer to the **CIS Configuration Editor User Guide**.

Important Note: A configuration can be implemented in any endpoint machine only if CIS has already been deployed to it. To know how to deploy CIS to endpoint machines, **click here**.

You can set protection for CIS in two ways.

Method 1 - Through shortcut in Right click options

1. Right click on the target computer (previously installed with CIS) from the list of computers in the Computers window.
2. Point to 'Internet Security' > 'Configuration' and select the required action parameter from the context sensitive menu as shown below.

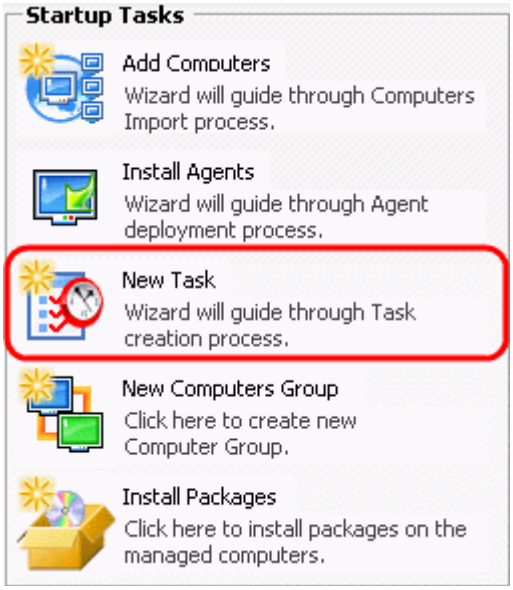


OR

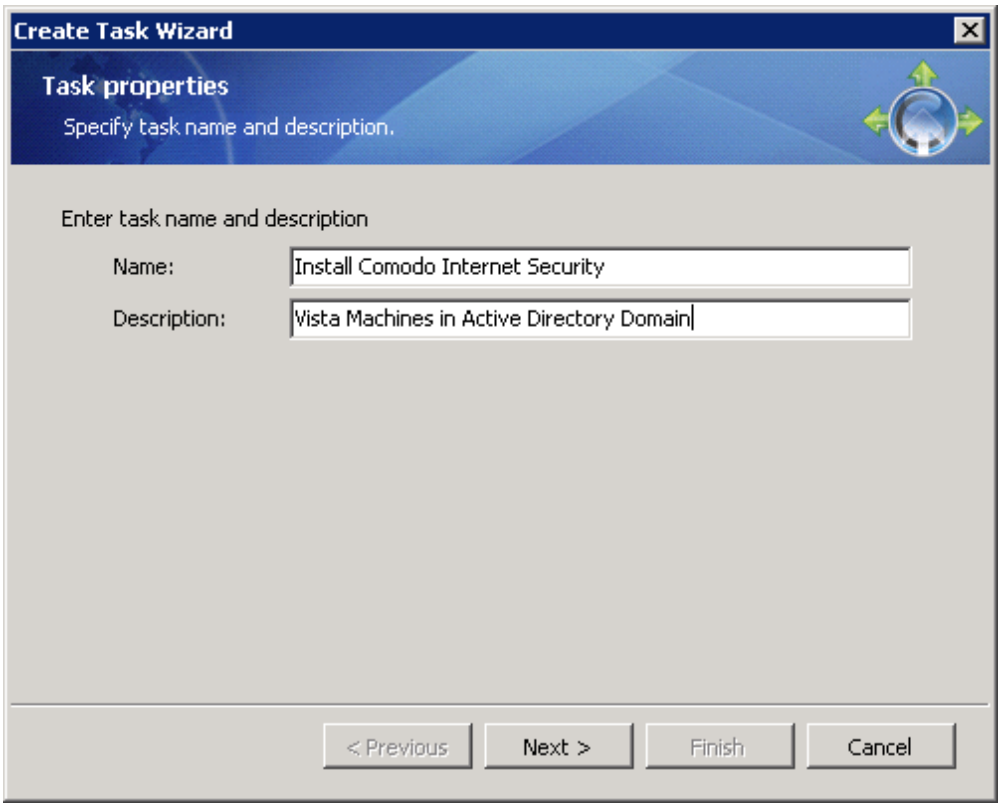
Method 2 - By creating a new task

To set protection for CIS, you need to create a new task with a sequence, containing the action 'CIS - Set predefined Config' and the required action parameter.

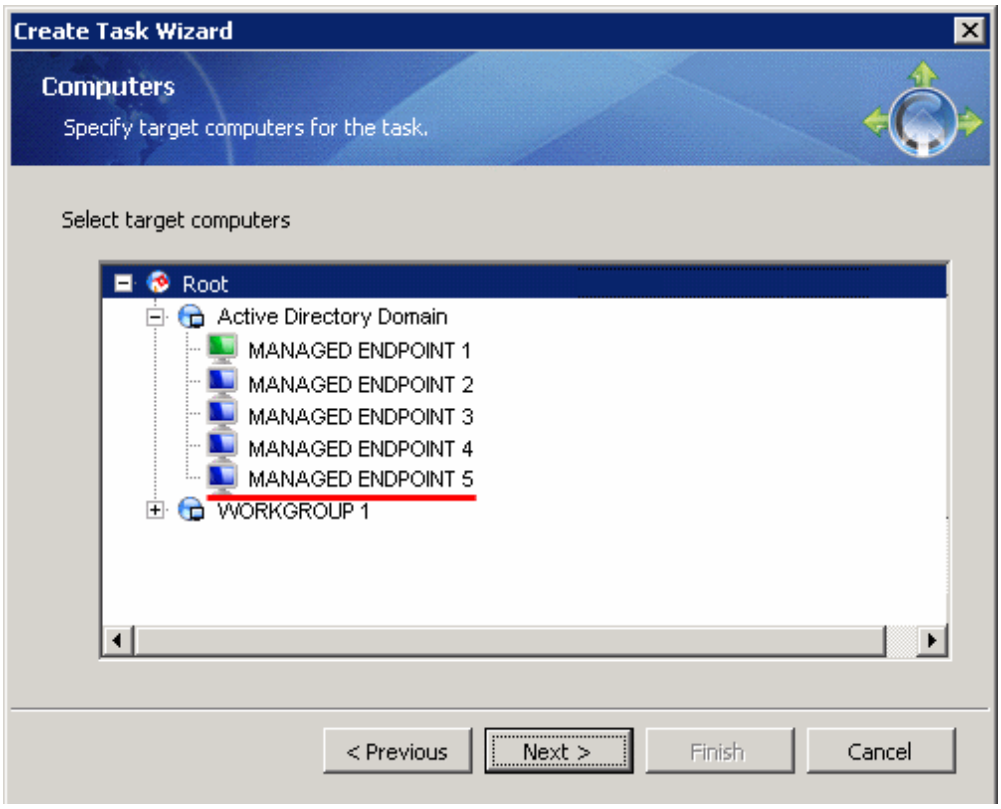
1. Click the link 'New Task' on the 'Start Page'.



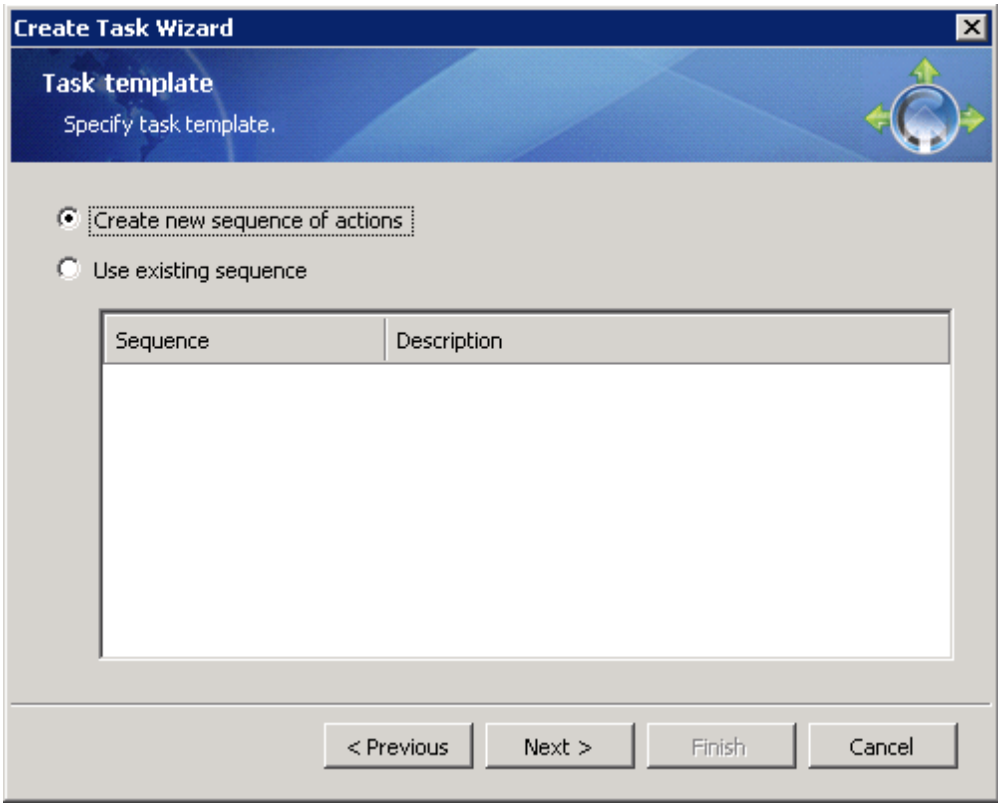
2. Type a name (mandatory) and a description (optional) for the new task in the 'Task Properties' dialog and click 'Next'.



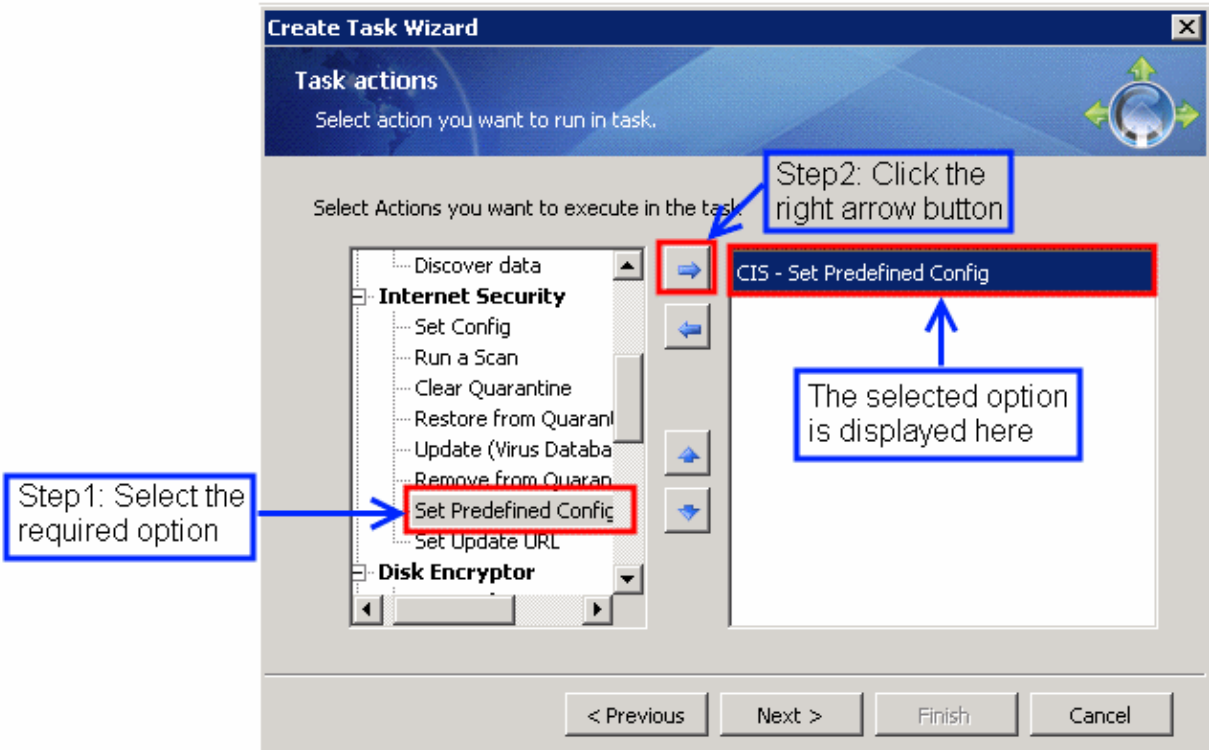
3. Select whether the new task has to be executed on to individual computers or a group of computers and then select the computers or groups from the displayed computer tree.



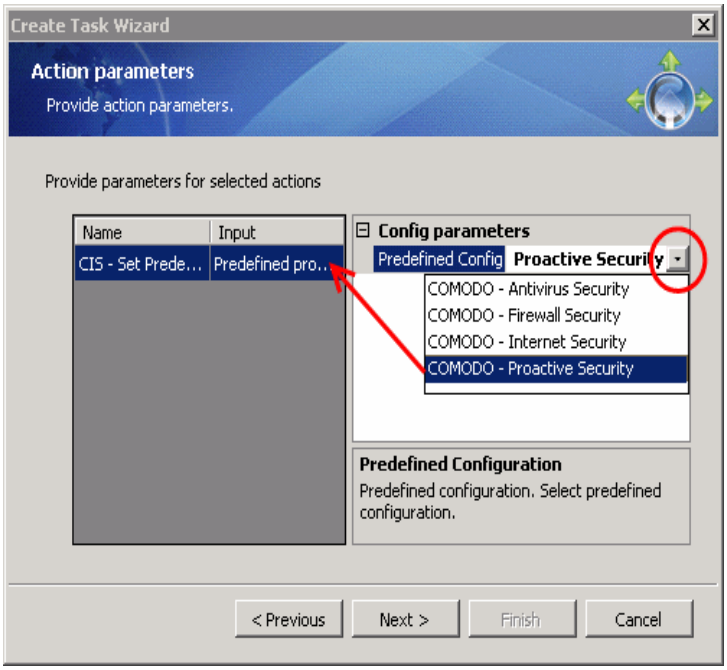
4. Select the radio button 'Create new sequence of actions' in the next step.



5. Select 'Set Predefined Config' under Internet Security category from the list of predefined actions displayed in the left pane of 'Task Actions' dialog, move it to the right pane by clicking the right arrow and click 'Next'.



6. Select the CIS Preset Config parameter in the next step.

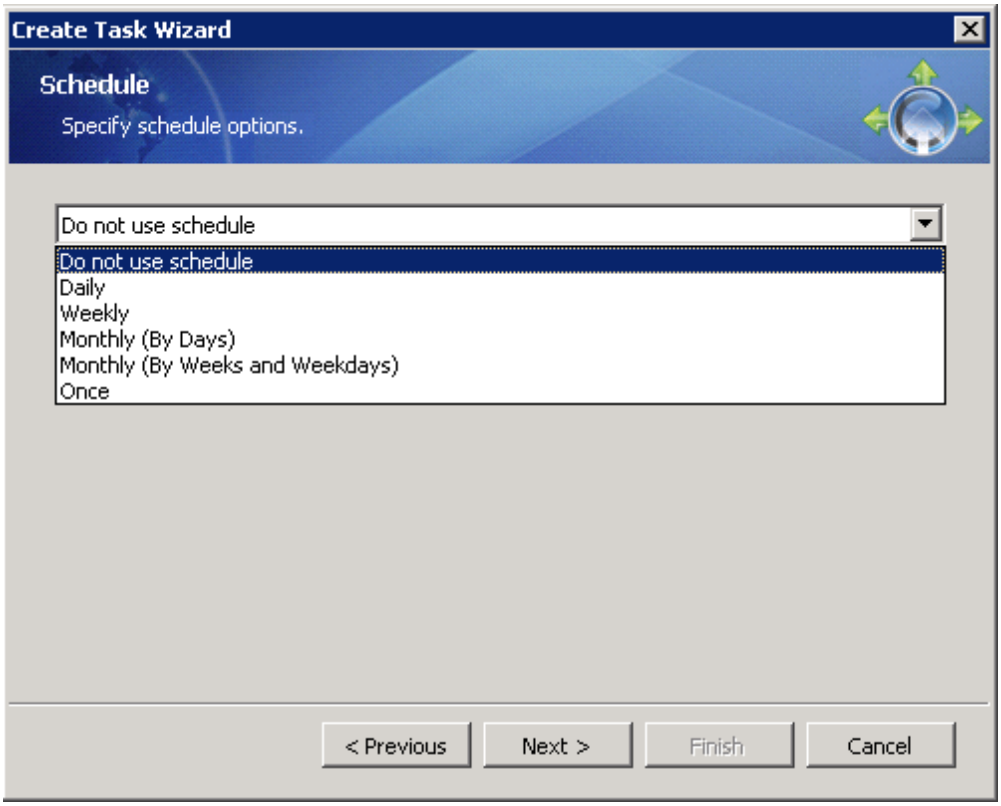


7. Click at the right end of the 'Predefined Config' text field and select the required Predefined Configuration from the four options in the drop-down menu and click 'Next'.

CIS - Predefined Configurations	
Option	**Description**
COMODO - Endpoint	**COMODO - Endpoint Security** - This profile has been especially designed to provide the perfect combination of security and usability for

Security	endpoint computers. • Firewall is set to "Safe mode" • Defense+ is set to "Safe mode" • Image Execution Control is set to "Normal" • Computer Monitor/Disk/Keyboard/DNS Client access/Window Messages are monitored • Defense+ is tuned to prevent infection of the system • Antivirus is fully enabled • Untrusted applications are automatically sandboxed
COMODO - Antivirus Security	Note - 'Antivirus Security' is a legacy profile that will only work with CIS 3.x. If you have CIS 4.x installed then do not use this profile (the task will fail). This profile is recommended if you chose to install *only* the antivirus component of CIS 3.x on a target machine while configuring the 'Install Package' Action (more specifically, if you left the Argument field blank for the CIS package). See 'The Package Management Window' if you would like to read more about Packages. This configuration of CIS implements the following settings: • Optimum protection settings for Defense+ • Image Execution Control is disabled. • Computer Monitor/Disk/Keyboard/DNS Client access/Window Messages are NOT monitored. • Only commonly infected files/folders are protected against infection. • Only commonly exploited COM interfaces are protected. • Defense+ is tuned to prevent infection of the system while creating least number of Defense+ pop-up alerts • Antivirus is fully enabled
COMODO - Firewall Security	This profile is recommended if only the firewall component of CIS needs to be installed on a target machine while configuring the 'Install Package' Action. TThis configuration of CIS implements the following settings: • Firewall is set to Safe mode • Optimum protection settings for Defense+ • Image Execution Control checks only applications that are not started manually by the user. • Computer Monitor/Disk/Keyboard is NOT monitored. • Only commonly infected files/folders are protected against infection. • Only commonly exploited COM interfaces are protected. • Defense+ is tuned to prevent infection of the system and detect Internet access request leaks even if it is infected. Untrusted applications are not sandboxed. They will still be blocked at the point of execution but will generate a Defense + alert instead of being sandboxed.
COMODO - Internet Security	This profile is recommended if the full CIS product (both Firewall and Antivirus components) needs to be installed on a target machine while configuring the 'Install Package' Action. This configuration of CIS implements the following settings:

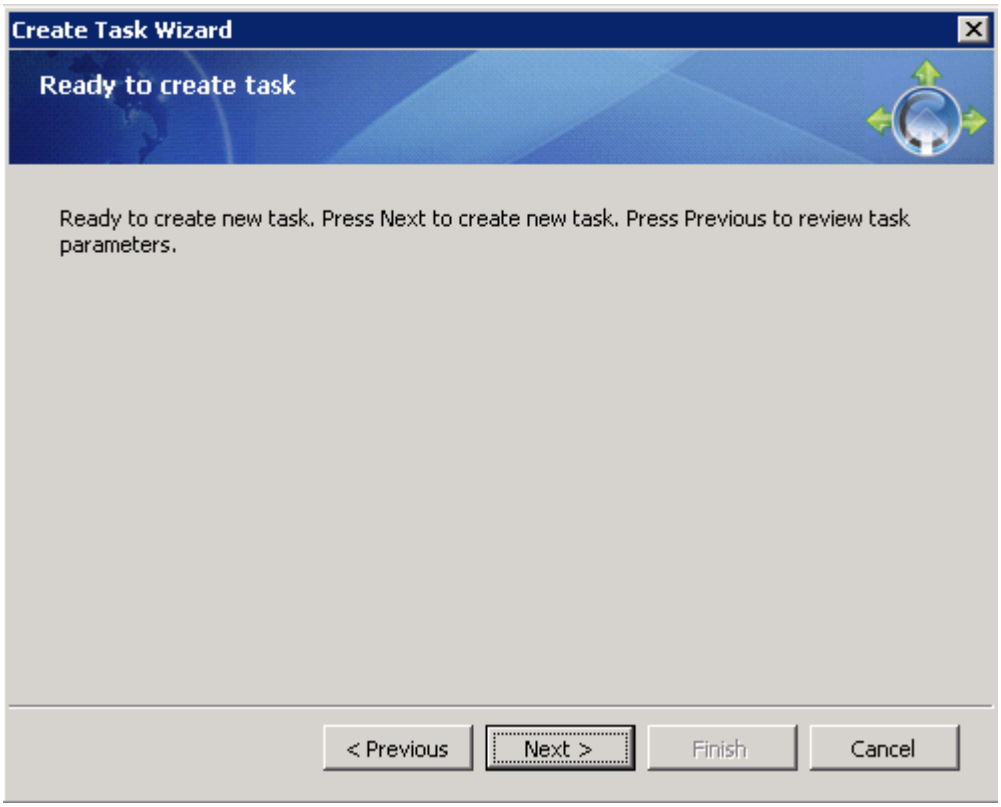
	• Firewall is set to 'Safe' mode • Defense+ is set to 'Safe' mode • Image Execution Control is disabled. • Computer Monitor/Disk/Keyboard/DNS Client access/Window Messages are NOT monitored. • Only commonly infected files/folders are protected against infection. • Only commonly exploited COM interfaces are protected. • Defense+ is tuned to prevent infection of the system. • Untrusted applications are automatically sandboxed
COMODO - Proactive Security	This configuration provides the highest level of protection for endpoint machines by enabling all possible security features within the suite. This profile is recommended to enable the highest security settings. This configuration of CIS implements the following settings: • Firewall is set to Safe mode • Maximum protection settings for Defense+. All possible protections are activated and all critical COM interfaces and files are protected • Antivirus is fully enabled • Untrusted applications are automatically sandboxed



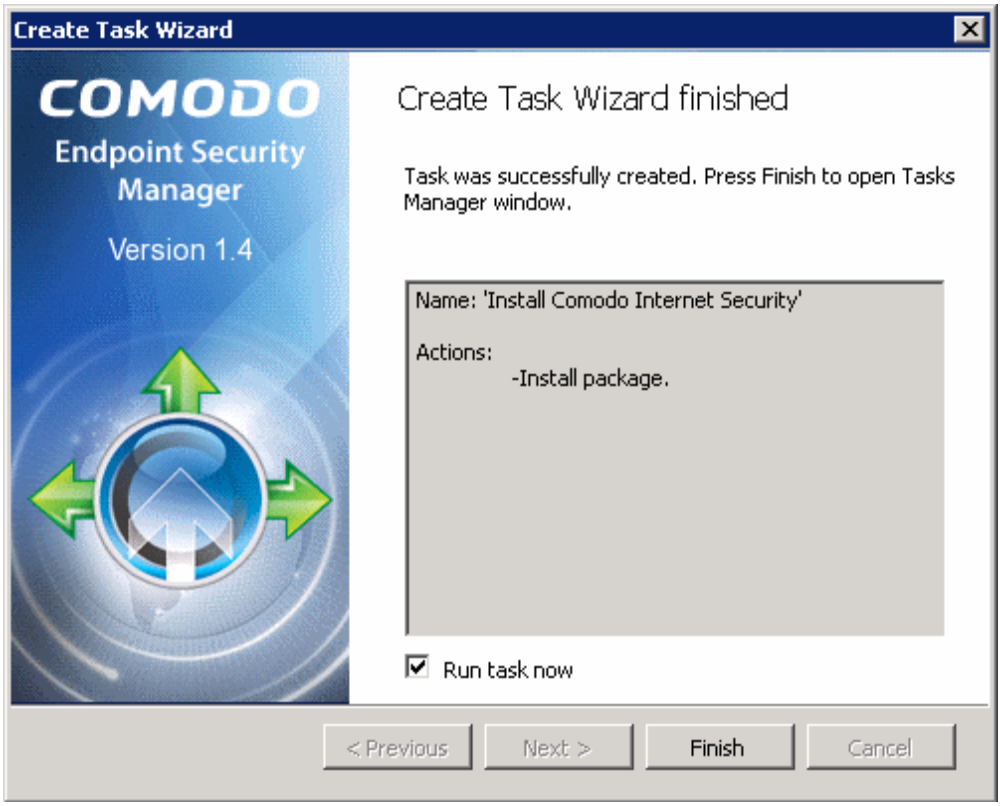
8. Schedule the task (optional). If you wish to timetable this task to run at regular intervals (or to delay it's execution until a later time) then select one of the options from the drop down menu. On the last step of the wizard, you will be given the opportunity to run the task immediately in addition to any schedule you may have set up here. To skip this stage, select 'Do not use schedule' from the drop-down menu and click 'Next'.

9. Click 'Next' on the confirmation dialog to confirm your choices up until this point and to create the Task. After clicking 'Next', the Task will be saved and can be accessed at any time in the future via the Task Manager window. Click 'Next'

to continue to Task finalization.



10. To immediately execute this task, leave the 'Run task now' checkbox selected and click 'Finish'. This will install CIS with the maximum security, 'Proactive Defense' configuration on the selected endpoints. If you do not wish to run it immediately, deselect the box and click 'Finish'.



4. The Custom Configuration Editor

The Custom Configuration Editor allows administrators to configure CIS security settings as per their requirements.

Notes:

- A configuration can only be implemented on endpoint machines with CIS installed. To know how to deploy CIS to endpoint machines, **click here**
- After installation of CIS, administrators **MUST** deploy a CIS configuration to activate the software. This can be a **preset configuration** or a custom configuration (this chapter)
- If you wish to modify the configuration of CIS already running on an endpoint then right click on the machine and select 'Custom....'. This will fetch the configuration already in effect and open it in the editor
- Once you are satisfied with your configuration in the editor, click the 'OK' button to save this configuration within the Task you are setting up. If you wish to export this configuration to a .xml file then select 'File > Save as...' at the top right of the editor (for example, to import into another Task at a later date).

There are three easy ways to access the CIS Configuration Editor using the CIS Set Config action:

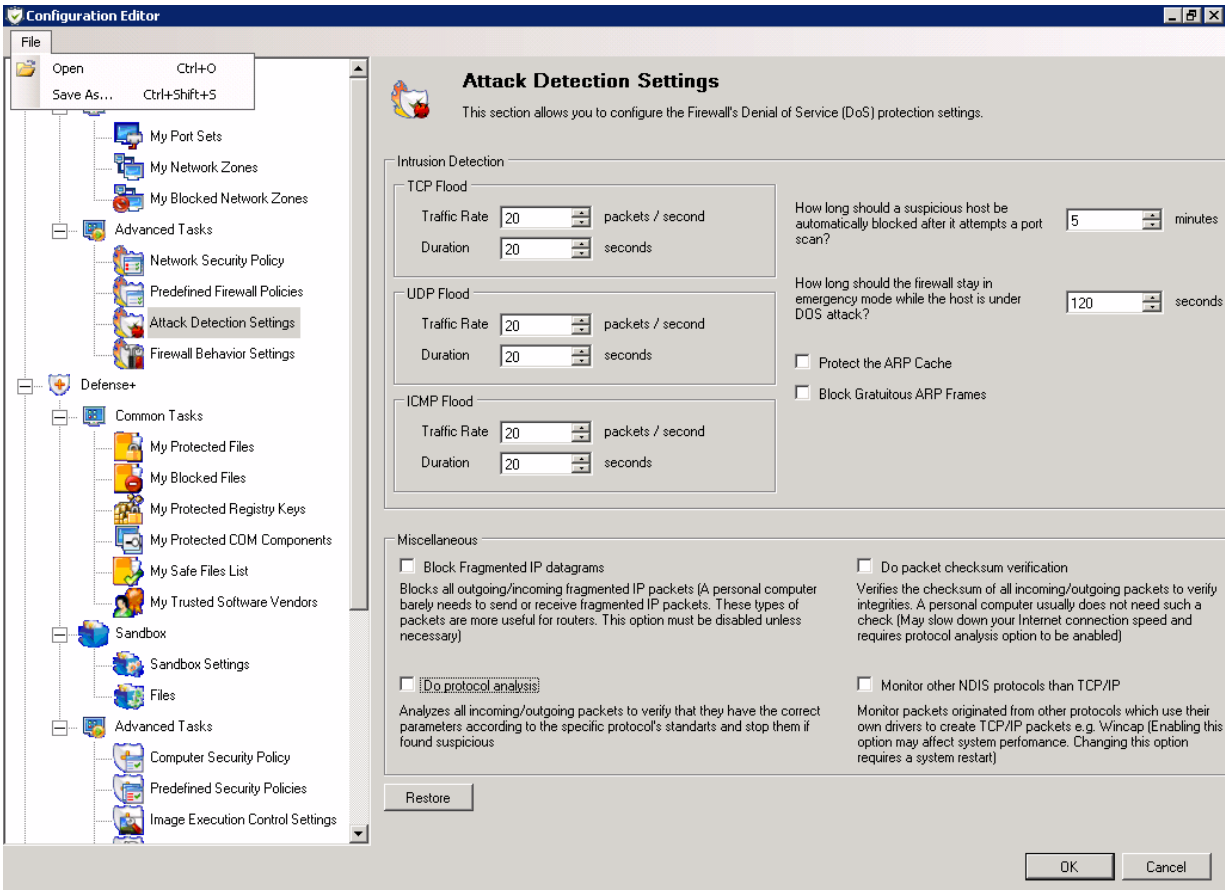
1) By Right Clicking on an imported computer. Right click on the target computer (previously installed with CIS) from the list of computers in the Computers window. Point to 'Internet Security' > 'Configuration' and select 'Custom' from the context sensitive menu. This will open the current CIS configuration in the editor.

OR

2) By using the 'New Task' wizard. Click 'New Task' on the Start Page; create a name and description for the Task ; select the target computer(s); select 'New Sequence' ; select 'Internet Security' > 'CIS Set Config' as the Task Action then click 'Next'. Now select 'Config' under the 'Config parameters' section and then click the ellipsis button (...) on the right to open the CIS Configuration Editor. This will open a blank configuration profile in the editor.

OR

3) By creating a new sequence manually. Open the 'Sequence Manager', click the 'Add' icon. Again click the 'Add' icon in the 'New Sequence' window, select 'CIS Set Config' option and click OK . Now select 'Config' under the 'Config parameters' section and then click the ellipsis button (…) on the right to open the CIS Configuration Editor.This will open a blank configuration profile in the editor.



The CIS Configuration Editor

General Note: Unlike the standalone (home) version of CIS, the CESM version is controlled remotely and is not directly accessible from endpoint machines. Administrators looking to familiarize themselves with the workings of CIS (and to gauge the effect of the settings that they implement using this editor) may want to consider first installing the standalone version of CIS first. This can be downloaded from **http://personalfirewall.comodo.com**.

The CIS Editor is split into five main configuration areas - Firewall , Defense + , Anti-Virus , Miscellaneous and Common Settings

Firewall

The Firewall center allows the administrator to quickly and easily configure all aspects of the Firewall. It offers the highest levels of security against inbound and outbound threats, stealth the computer's ports against hackers and blocks malicious software from transmitting confidential data over the Internet.

Defense+

Defense+ is a host intrusion prevention system that constantly monitors the activities of all executable files on a PC. Defense+ also protects against data theft, computer crashes and system damage by preventing most types of buffer overflow attacks.

Antivirus Overview

Comodo Antivirus leverages multiple technologies, including Real-time / On-Access Scanning and Manual / On Demand Scanning and to immediately start cleaning or quarantining suspicious files from the hard drives, shared disks, emails, downloads and system memory. The interface also

allows administrator to create custom scan profiles which can be re-used across all scan types and features full event logging, quarantine and file submission facilities.

Common

The Common module helps to create common groups, the entities of which are called in several interfaces within CIS Configuration Editor.

Miscellaneous Overview

The Miscellaneous section allows the administrator to configure connectivity settings to Comodo's Proxy servers.

Use the bookmarks on the left to jump to the particular section you need help on.

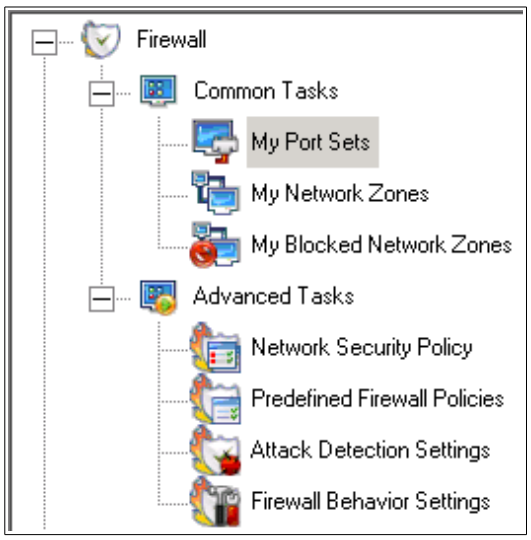
4.1. Firewall Overview

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

The Firewall center allows the administrator to quickly and easily configure all aspects of the Firewall.

It can be accessed by clicking on the Firewall Shield button 

It is divided into two sections: **Common Tasks** and **Advanced Tasks**



4.1.1 Common Tasks

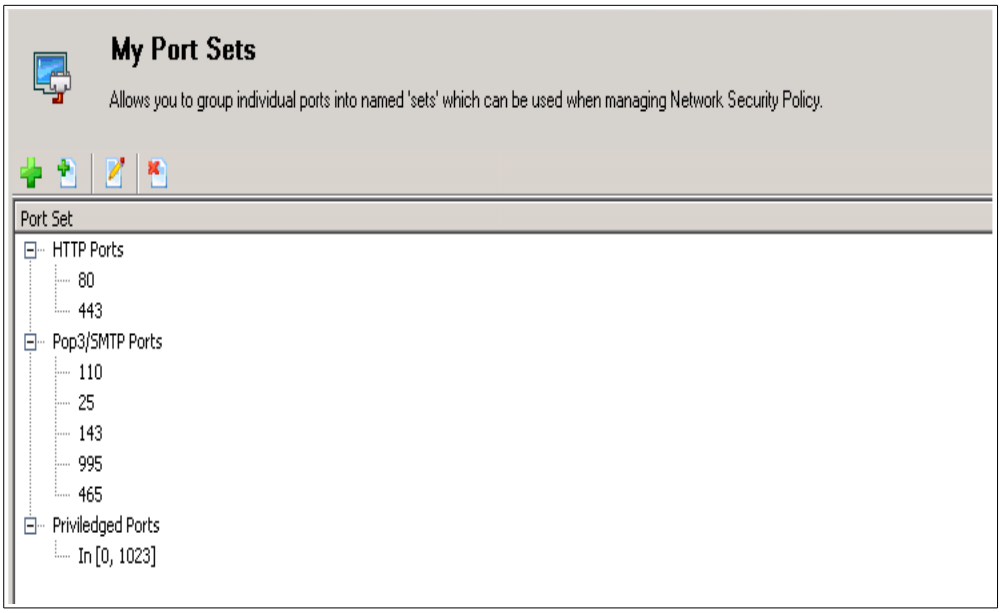
'Common Tasks' helps to create rules for applications and network connections through a series of shortcuts and wizards. Click on the links below for detailed explanations of each area in this section.

- **My Port Sets**
- **My Network Zones**
- **My Blocked Network Zones**

4.1.1.1 My Port Sets

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

- Click on **My Port Sets** in Firewall > Common Tasks to open 'My Port Sets' interface.



Note: The name of the Port Set is shown above the actual port numbers that belong to that set. The default port sets shipped with Comodo Internet Security are:

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

Once opened, the 'My Port Sets' window enables administrators to add new port sets and ports, edit and delete port sets and ports.

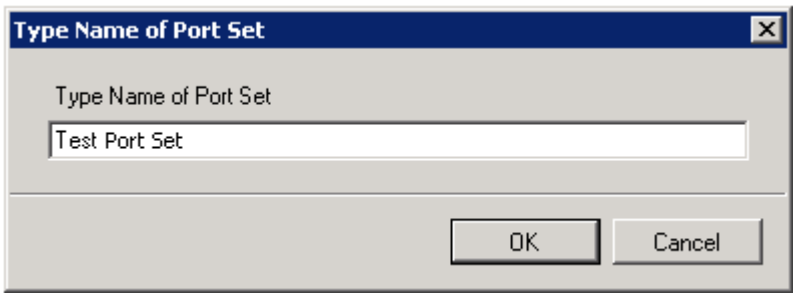
Window Specific Controls - My Port Sets		
Menu Element	**Element Icon**	**Description**
Add New Port Set		Enables the administrator to add a New Port Set
Add New Port		Enables the administrator to add a single port or a port range to the selected Port Set
Edit		Enables the administrator to edit the selected Port Set / Port
Remove		Removes the selected Port Set / Port

To Create a new Port Set

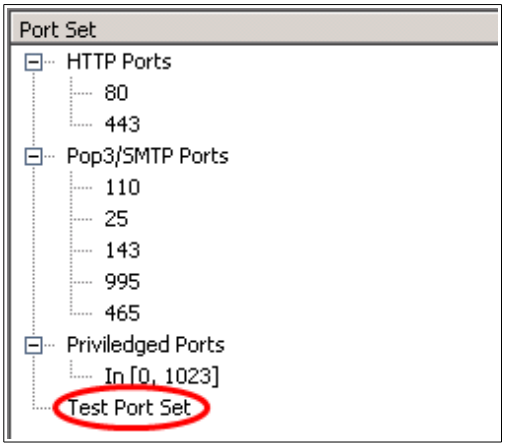
- Define a name for the Port Set.
- Select the port numbers that needs to be added to this named set.

To Define a name for the Port Set

1. Click the  icon in the 'My Port Sets' window. The naming dialog box is displayed.

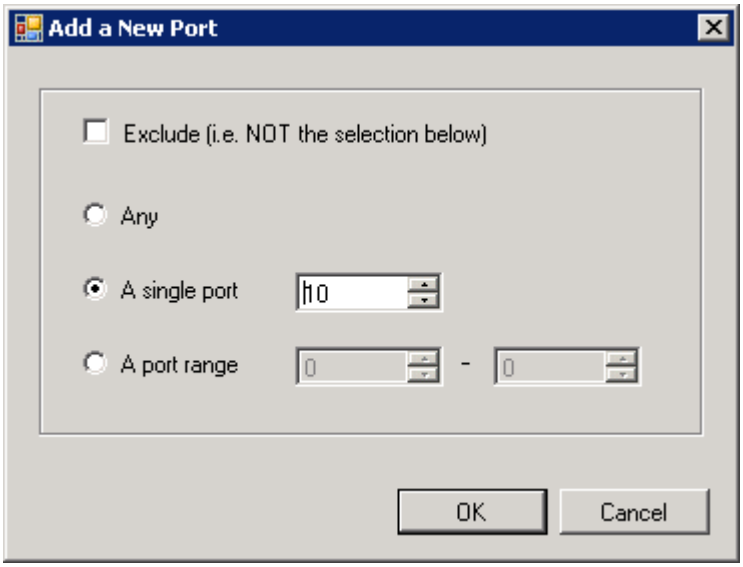


2. Type a name for the port set. In the image above, *Test Port Set* is taken as an example.
3. Click OK to confirm the name. The name of the new port set is added to the Port Set list:



To Define Port numbers for the Port Set

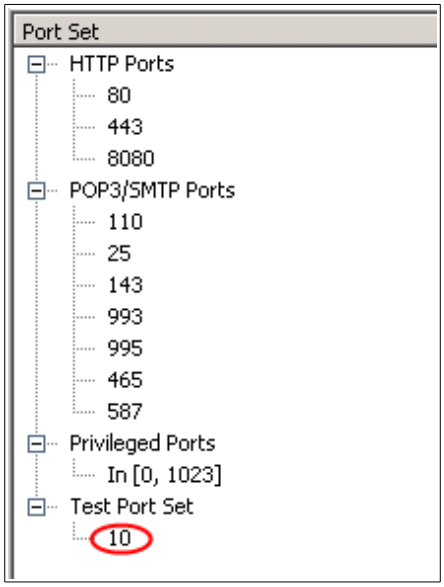
1. Select the Port Set for which the ports are defined and click the  icon in the 'My Port Sets' window. The 'Add a New Port' dialog box is displayed.



2. Add a New Port by selecting

- **Any,** to choose all ports;
- **A single port** and defining the required port in the combo box beside;
- **A port range** and typing the start and end port numbers in the respective combo boxes.

3. Click **OK** to confirm. The New Port Set displays the added ports in the main list.

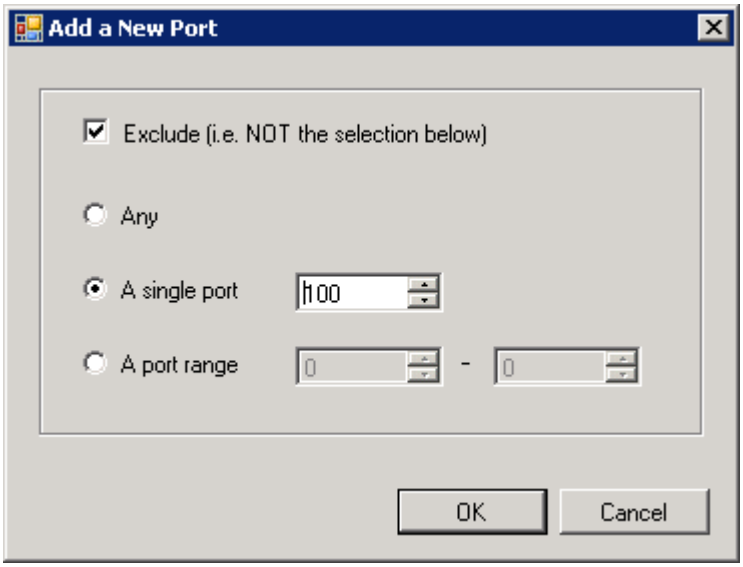


Note: To add more ports to this Port Set or to an existing Port Set, select the appropriate Port Set and repeat the process from the fourth step.

To exclude a Port number from a Port Set

Note: The **Exclude** option is used to exclude a port number or a range of port numbers from the selected Port Set. This ensures that the excluded port is not used as a part of the selected Port Set.

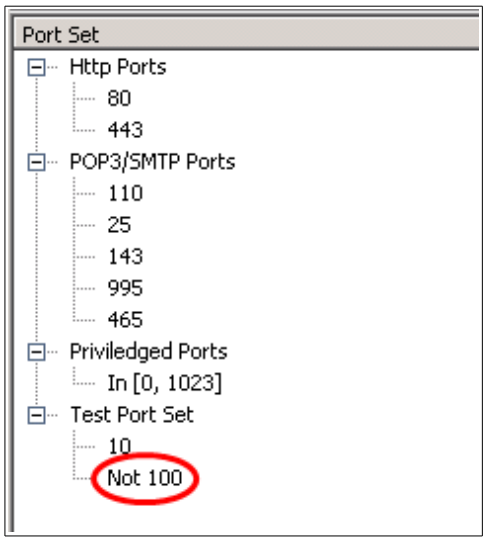
1. Select the Port Set for which the ports are to be excluded and click the icon in the 'My Port Sets' window. The 'Add a New Port' dialog box is displayed.



2. Select 'A single port' or 'A port range' option to enable the Exclude checkbox.

Note: The **Exclude** option remains disabled if **Any** option is selected in the 'Add a New Port' dialog box.

3. Enter the single port or the port range in the respective combo boxes.
4. Select the Exclude checkbox and click **OK** to confirm. The excluded port number is displayed in the main Port Set list:



To Edit the name of an existing Port Set

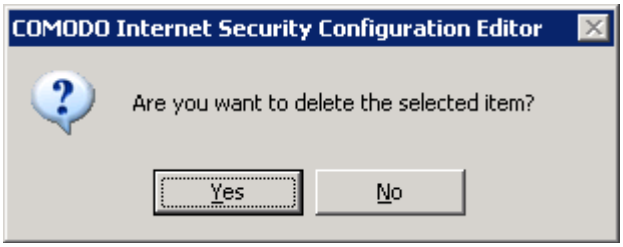
1. Select the name of the Port Set in the list (e.g. HTTP Ports) and click the icon to bring up the 'Edit Port Set Name' dialog box.
2. Modify the name and click **OK** to confirm.

To Edit the existing Port numbers in a Port Set

1. Select the Port number in the appropriate Port Set and click the icon to bring up the 'Edit Port' dialog box.
2. Modify the Port number and click **OK** to confirm.

To Delete a Port Set or a Port number

1. Select the required Port Set or Port number and click the icon. The following confirmation dialog box is displayed.



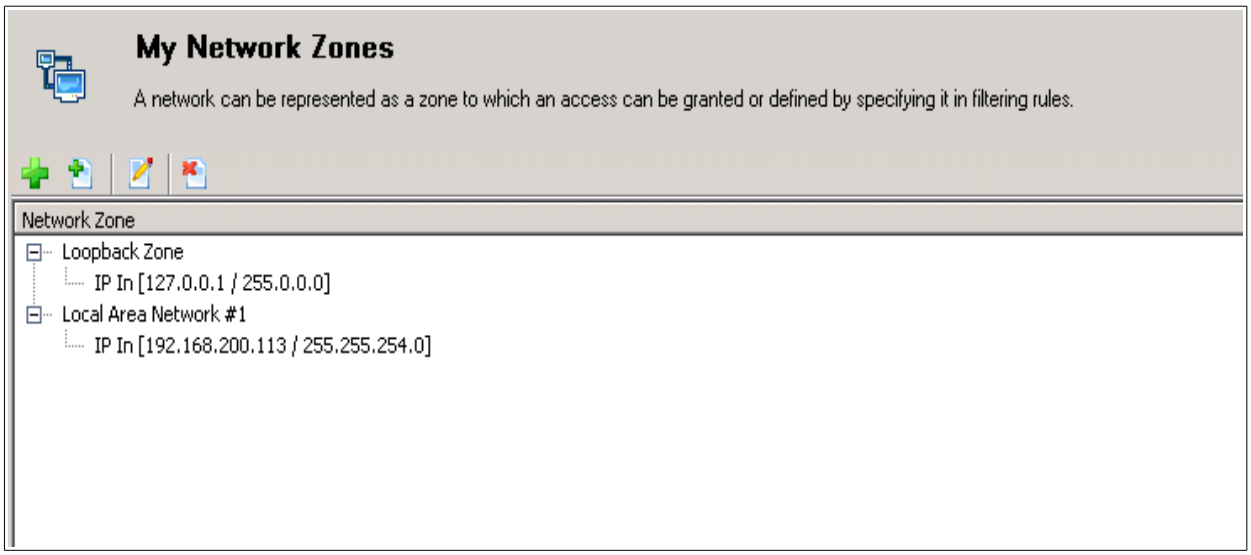
2. Click **Yes** to delete the selected item.

4.1.1.2 My Network Zones

A computer network is a connection between computers through a cable or any type of wireless connection. It is highly useful in sharing information and devices between one computer and another within the network. Obviously, there are certain computer networks where the administrator has to grant access. Conversely, there may be other networks where the administrator want to restrict communication with or even block the network entirely.

Comodo Firewall allows the administrator to define 'Network Zones' and to specify the access privileges of these zones. A 'Network Zone' can consist of an individual machine or a network of thousands of machines to which access can be granted or denied, irrespective of whether the machines are connected to the internet or within an intranet.

- Click on **My Network Zone** in Firewall > Common Tasks to open 'My Network Zone' interface.



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

Note 2: A network zone can be designated as 'Blocked' and denied access by using the '**My Blocked Network Zones**' interface. (An example would be a known spyware site)

Note 3: An application can be assigned specific access rights to and from a network zone when defining an **Application Rule**. Similarly, a custom **Global Rule** can be assigned to a network zone to all activities from a zone.

Note 4: By default, Comodo Firewall automatically detects any new networks (LAN, Wireless etc). This can be disabled in the **Miscellaneous - Settings** area of the firewall.

Once opened, the 'My Network Zones' window enables administrators to add new network zones and IP addresses, edit and delete network zones and IP address.

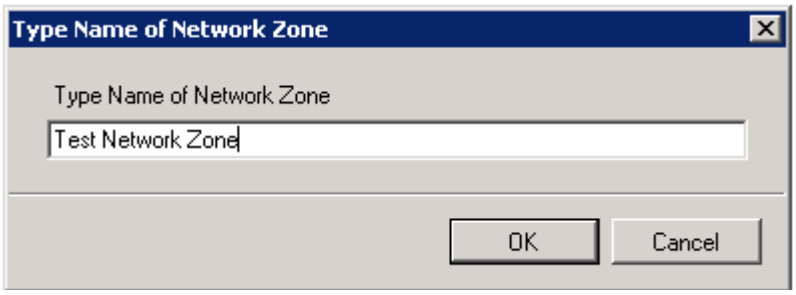
Window Specific Controls - My Network Zones		
Menu Element	**Element Icon**	**Description**
Add New Network Zone		Enables the administrator to add a New Network Zone
Add New Address		Enables the administrator to add a single IP address, a range of IP Addresses, an IP address mask, a host name or a MAC address to the selected Network Zone
Edit		Enables the administrator to edit the selected Network Zone / IP Address
Remove		Removes the selected Network Zone / IP Address

To Create a New Network Zone

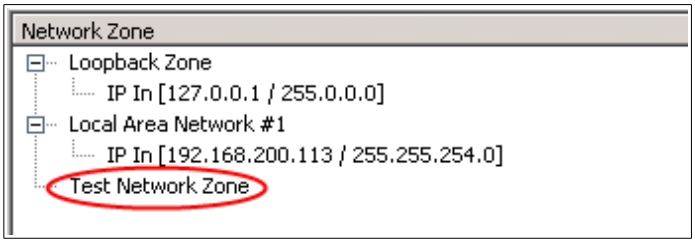
- Define a name for the Network Zone.
- Select the IP Addresses to be included in this zone.

To Define a name for the Network Zone

1. Click the icon in the 'My Network Zones' window. The naming dialog box is displayed.

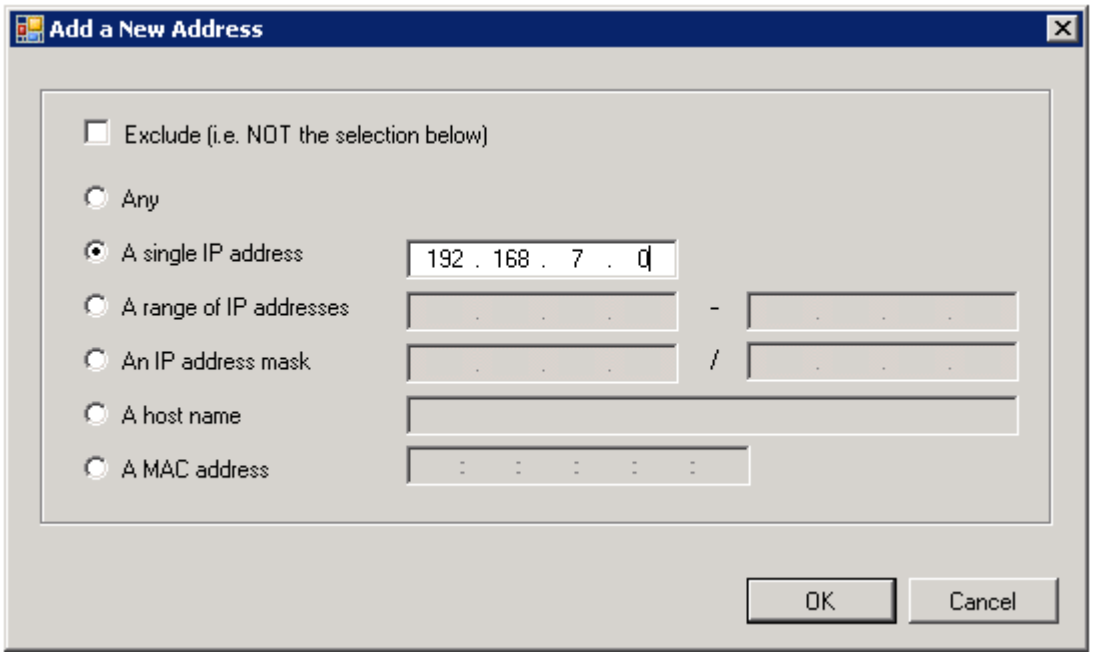


2. Type a name that relatively describes the Network Zone being created.
3. Click **OK** to confirm the zone name. The name of the new zone is added to the Network Zones list.

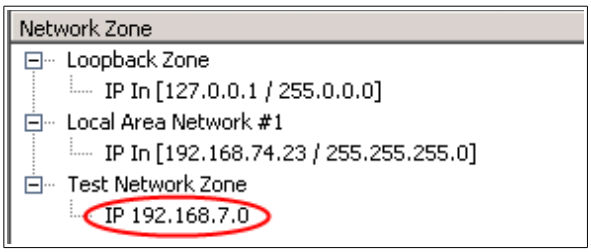


To define IP Addresses for the zone

1. **Select** the Network Zone and click the icon from the menu. The 'Add a New Address' dialog box is displayed.



2. Select the required option. This dialog box allows the administrator to specify an address by typing an IP address; an IP range; an IP address mask; a host name or a MAC address.
3. Click **OK** to confirm. The address is displayed under the selected network zone.

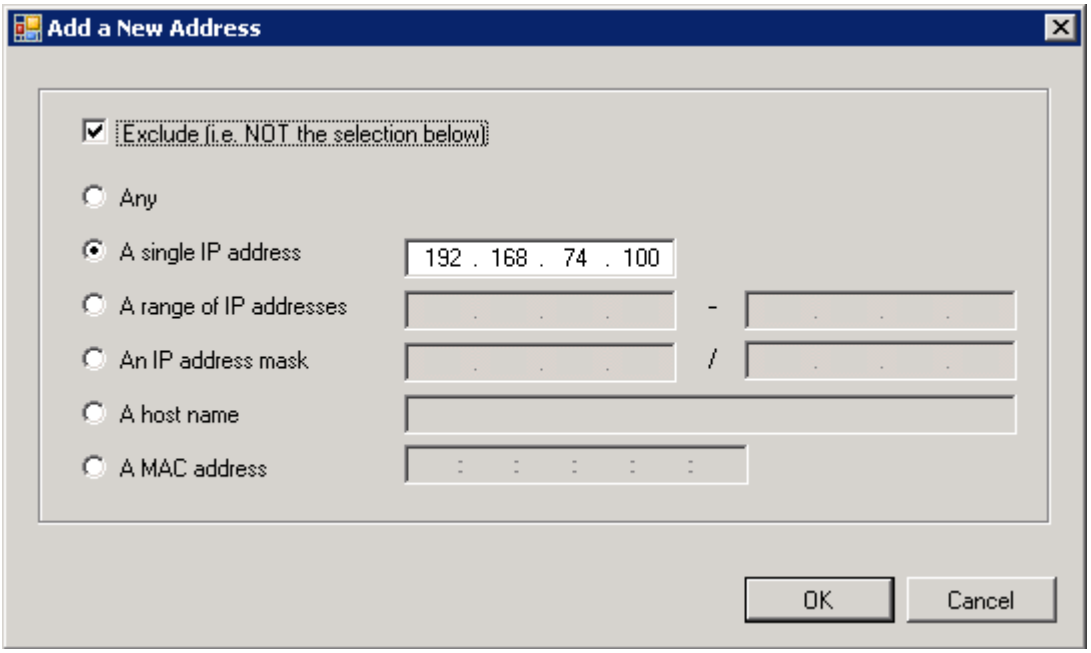


Note: To add more IP Addresses to this Network Zone or to an existing Network Zone, select the appropriate zone and repeat the process from the fourth step.

To exclude a IP Address from a Network Zone

Note: The **Exclude** option is used to exclude IP Addresses from the selected Network Zone. This ensures that the excluded IP Addresses are not used as a part of the selected Network Zone.

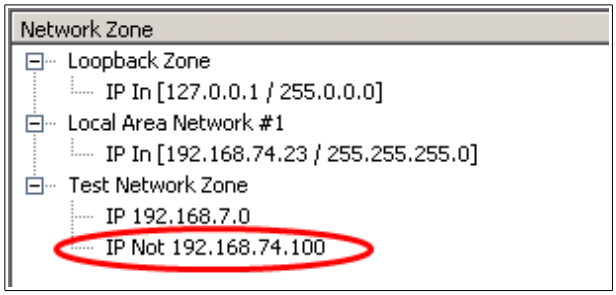
1. Select the Network Zone for which IP Addresses are to be excluded and click the icon in the 'My Network Zones' window. The 'Add a New Address' dialog box is displayed.



2. Select the required option to enable the **Exclude** checkbox.

Note: The **Exclude** option remains disabled if **Any** option is selected in the 'Add a New Address' dialog box.

3. Enter the **relevant** IP Addresses in the respective combo boxes.
4. Select the **Exclude** checkbox and click **OK**. The excluded IP address is displayed in the main Network Zone list:



To edit the name of an existing Network Zone

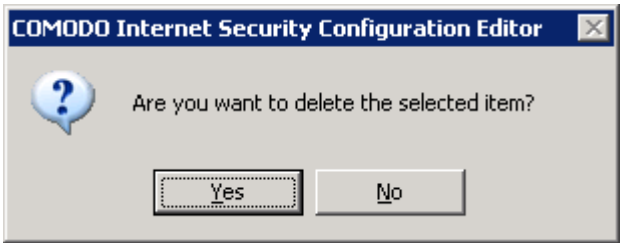
1. Select the name of the zone in the list (e.g. Test Network Zone) and click the icon to bring up the 'Edit Network Zone Name' dialog box.
2. Modify the name and click **OK** to confirm.

To edit the existing IP Address in a Network Zone

1. Select the IP Address in the appropriate Network Zone and click the icon to bring up the 'Edit Address' dialog box.
2. Modify the Port number and click **OK** to confirm.

To delete a Network Zone or IP Address

1. Select the required Network Zone or IP Address and click the icon. The following confirmation dialog box is displayed.



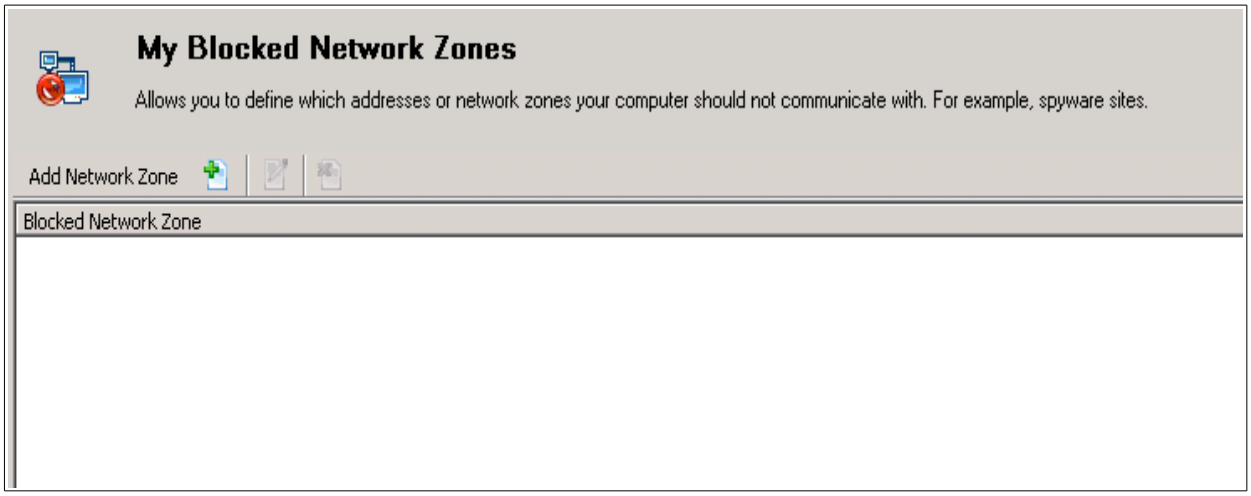
2. Click **Yes** to delete the selected item.

4.1.1.3 My Blocked Network Zones

A computer network helps to share information and devices between computers within the network. Obviously, there are certain computer networks that are trustable to grant access to and unfortunately, there may be other, untrustworthy networks that needs to be restricted from communicating with - or even block entirely.

The 'My Blocked Network Zones' interface allows to deny access to a specific network by selecting a pre-existing network zone and designating it as blocked and also to define new IP addresses and designate it as blocked.

- Click **My Blocked Network Zones** in Firewall > Common Tasks to open 'My Blocked Network Zones' interface.



Note 1: A zone must be created before it can be blocked. To create a new zone go to '**My Network Zones**' interface.

Note 2: *Pre-existing* network zones cannot be reconfigured from this interface.

(e.g., to add or modify IP addresses). To change the settings of existing zones go to '**My Network Zones**' interface.

Once opened, the 'My Blocked Network Zones' interface enables administrators to call existing network zones; add, edit and delete new IP addresses that are created in this interface.

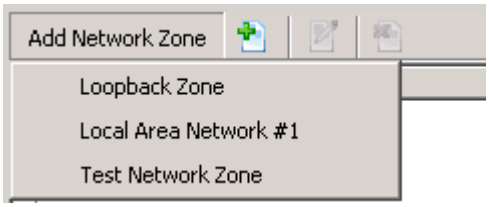
Window Specific Controls - My Blocked Network Zones		
Menu Element	**Element Icon**	**Description**
Add Network Zone	Add Network Zone	Enables the administrator to call an existing Network Zone
Add New Blocked Address		Enables the administrator to add a single IP address, a range of IP Addresses, An IP address mask, a host name or a MAC address to the Blocked Network Zone list
Edit		Enables the administrator to edit the newly added blocked IP Addresses
Remove		Removes the selected Network Zone / newly added blocked IP Address

To create a Blocked Network Zone

- Call an existing Network Zone to be blocked.
- Add the required IP address to be blocked.

To call a Network Zone

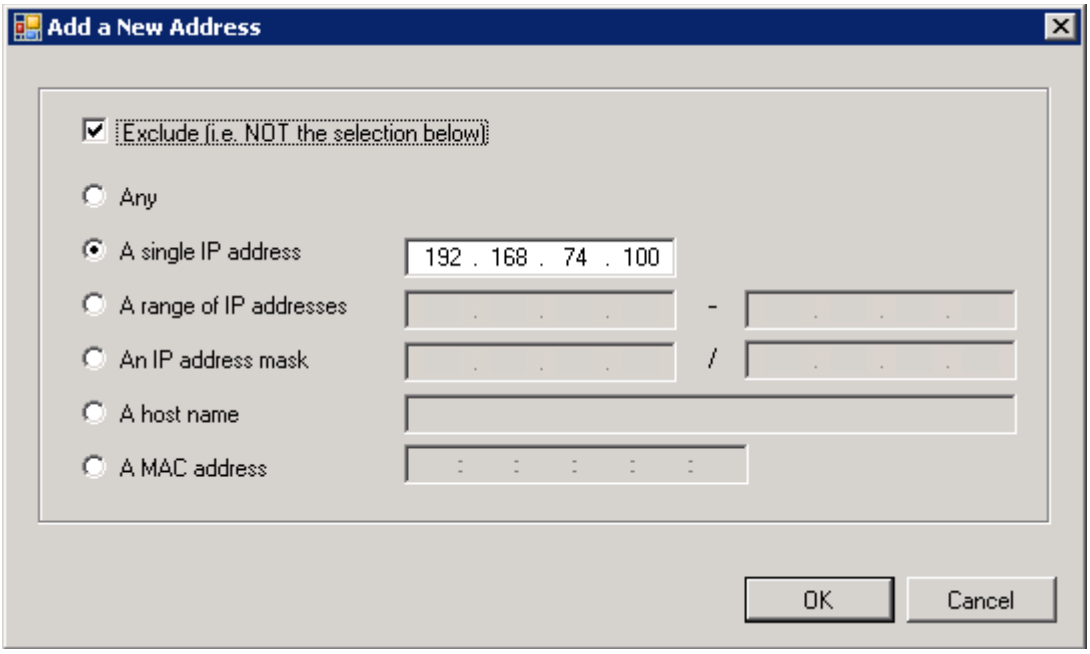
1. Click the Add Network Zone button in the 'My Blocked Network Zones' Interface. A list of existing Network Zones is displayed.



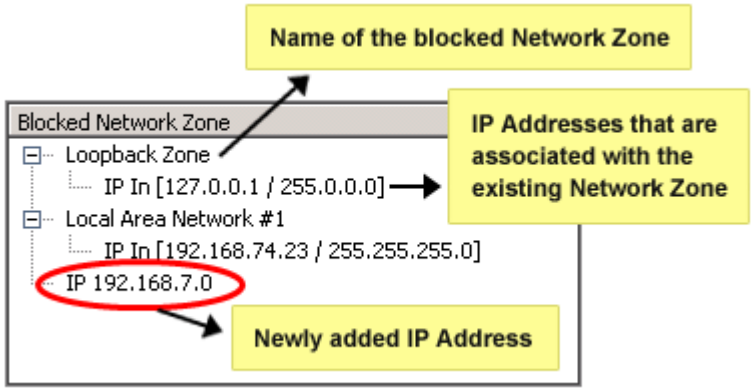
2. Click the required zone that needs to be blocked. The selected zone is displayed in the Blocked Network Zone list and all traffic intended for and originating from computer or devices in this zone is now blocked.
3. Repeat the procedure to add more zones to the blocked list.

To define IP Addresses to be blocked

1. Click the  icon from the menu. The 'Add a New Address' dialog box is displayed.



2. Select the required option. This dialog box allows the administrator to specify an address by typing an IP address; an IP range; an IP address mask; a host name or a MAC address.
3. Click **OK** to confirm. The IP address is displayed in the blocked list and all traffic intended to and originating from this IP Address is now blocked.

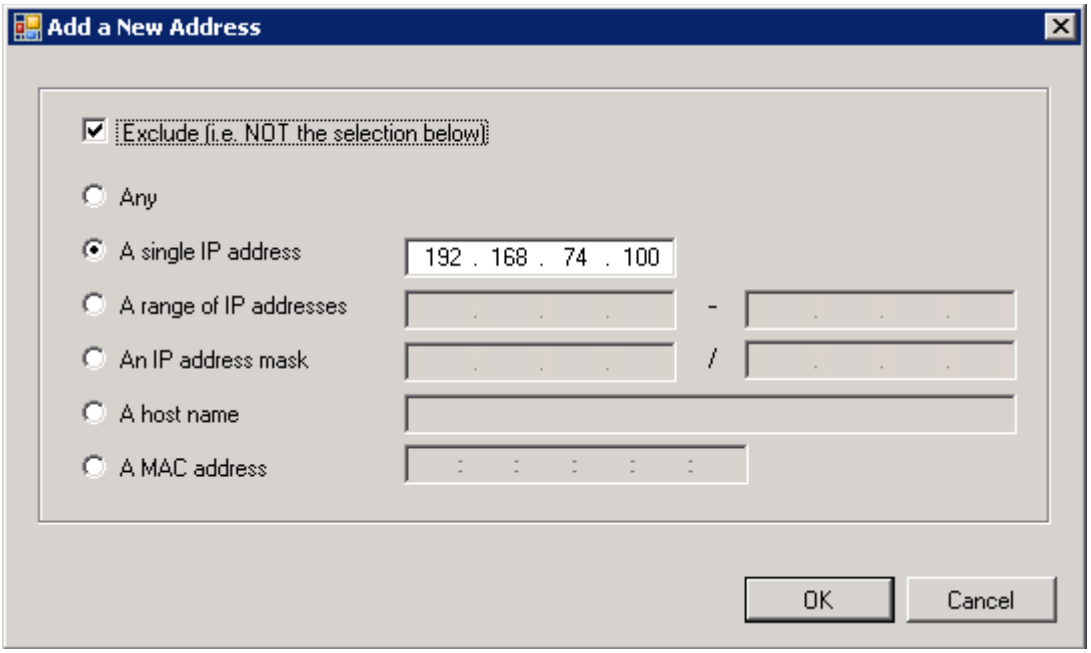


Note: To add more IP Addresses to the blocked list, repeat the procedure from the fourth step.

To exclude an IP Address from a Network Zone

Note: The **Exclude** option is used to exclude IP Addresses from the selected Blocked Network Zone. This ensures that the excluded Blocked IP Addresses are not used as a part of the selected Network Zone.

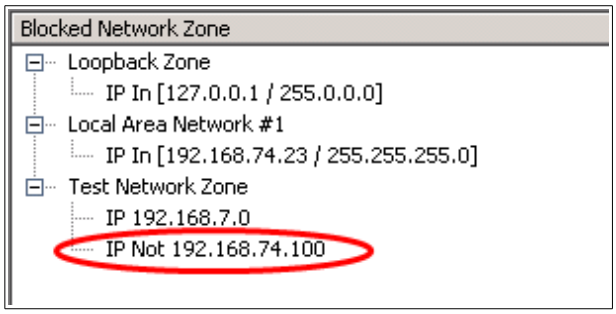
1. Select the Blocked Network Zone for which IP Addresses are to be excluded and click the icon in the 'My Network Zones' window. The 'Add a New Address' dialog box is displayed.



2. Select the required option to enable the **Exclude** checkbox.

Note: The **Exclude** option remains disabled if **Any** option is selected in the 'Add a New Address' dialog box.

3. Enter the relevant IP Addresses in the respective combo boxes.
4. Select the **Exclude** checkbox and click **OK**. The excluded IP address is displayed in the main Blocked Network Zone list:



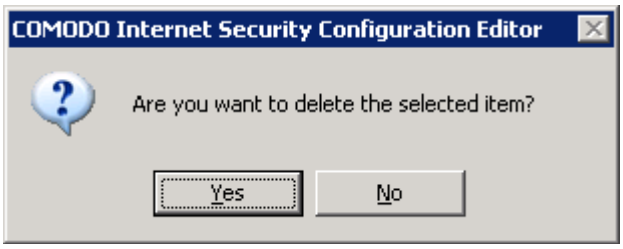
To edit an IP Address in the blocked list

1. Select the IP Address from the blocked list and click the icon to bring up the 'Edit Blocked Address' dialog box.
2. Modify the Port number and click **OK** to confirm.

Note: Only newly added IP Address can be edited in this interface. To modify IP Addresses in existing Network Zones, go to '**My Network Zones**' interface and edit the IP addresses.

To delete a Network Zone or IP Address

1. Select the required Network Zone or IP Address and click the icon. The following confirmation dialog box is displayed.



2. Click **Yes** to delete the selected item.

Special Note: Creating a blocked network zone implements a 'block all' **global rule** for the zone in question. However, unlike when a 'Trusted Zone' is created, this rule is not displayed or editable from the global rules tab of the Network Security Policy interface. This happens because only a few zones can be trusted and there is a potential to block many. The constant addition of such block rules would make the interface unmanageable for most administrators.

4.1.2 Advanced Tasks

'Advanced Tasks' enables more experienced administrators to define firewall policy and settings at an in-depth, granular level. Click on the links below for detailed explanations of each area in this section.

- **Network Security Policy**
- **Predefined Firewall Policy**
- **Attack Detection Settings**
- **Firewall Behavior Settings**

4.1.2.1 Network Security Policy

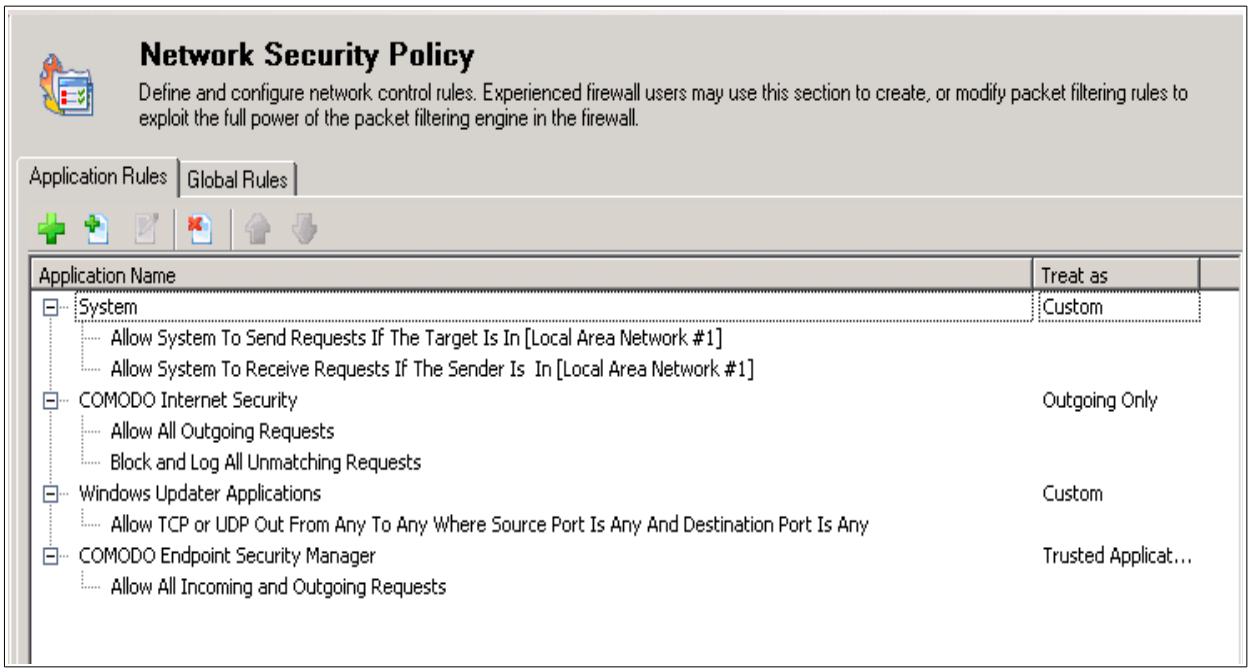
The Network Security Policy interface is the nerve center of Comodo Firewall and allows advanced administrators to configure and deploy traffic filtering rules and policies on an application specific and global basis.

- Click on **Network Security Policy** in firewall > Advanced Task to open the 'Network Security Policy' interface.

The interface is divided into two main sections - **Application Rules** and **Global Rules.**

The **Application Rules** tab allows administrators to view, manage and define the network and Internet access rights of *applications* in the system.

The **Global Rules** tab allows administrators to view, manage and define overall network policy that applies to the 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.

See **General Navigation** for a summary of the navigational options available from the main Network Security Policy interface.

See the section **' Application Rules'** for help to configure application rules and policies.

See the section **'Global Rules'** for help to configure global rules and to understand the interaction between global and application rules.

General Navigation Controls for Network Security Policy interface:

Window Specific Navigation Controls - Network Security Policy		
Menu Element	**Element Icon**	**Description**
Add New Group		Allows the administrator to add a new application to the list then create its policy in the Application Rules tab. **Note**:This icon is not available in the Global Rules tab.
Add New Rule		Allows the administrator to add a new rule to the selected policy.
Edit		Allows the administrator to edit the selected application policy / rule
Remove		Removes the selected policy / rule
Move Up		Raises the currently selected policy / rule up by one row in the priority list. Administrators can also re-prioritize policies or re-assign individual rules to another application's policy by dragging and dropping.
Move Down		Lowers the currently selected policy / rule down by one row in the priority list. Administrators can also re-prioritize policies or re-assign individual rules to another application's policy by dragging and dropping.

Application Rules

See **Overview of Policies and Rules** for an explanation of rule and policy structure and how these are represented in the main Application Rules interface.

See **Application Network Access Control interface** for an introduction to the rule setting interface.

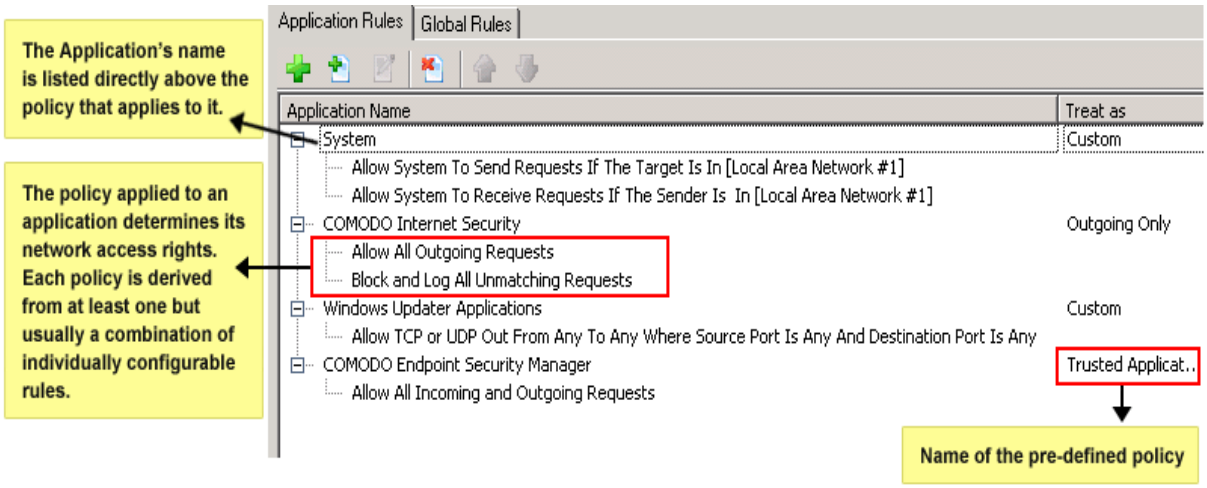
See **Creating and Modifying Network Policies** to learn how to create and edit network policies.

See **Understanding Network Control Rules** for an overview of the meaning, construction and importance of individual rules.

See **Adding and Editing a Network Control Rule** for an explanation of individual rule configuration.

Overview of Policies and Rules

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



To modify the **firewall policy** for an application:

- Double click on the application name to begin '**Creating or Modifying Network Policy**'

(OR)

- Select the application name and click the icon to begin '**Creating or Modifying Network Policy**'

To modify an **individual rule** within the policy:

- Double click on the specific rule to begin '**Adding and Editing a Network Control Rule**'

(OR)

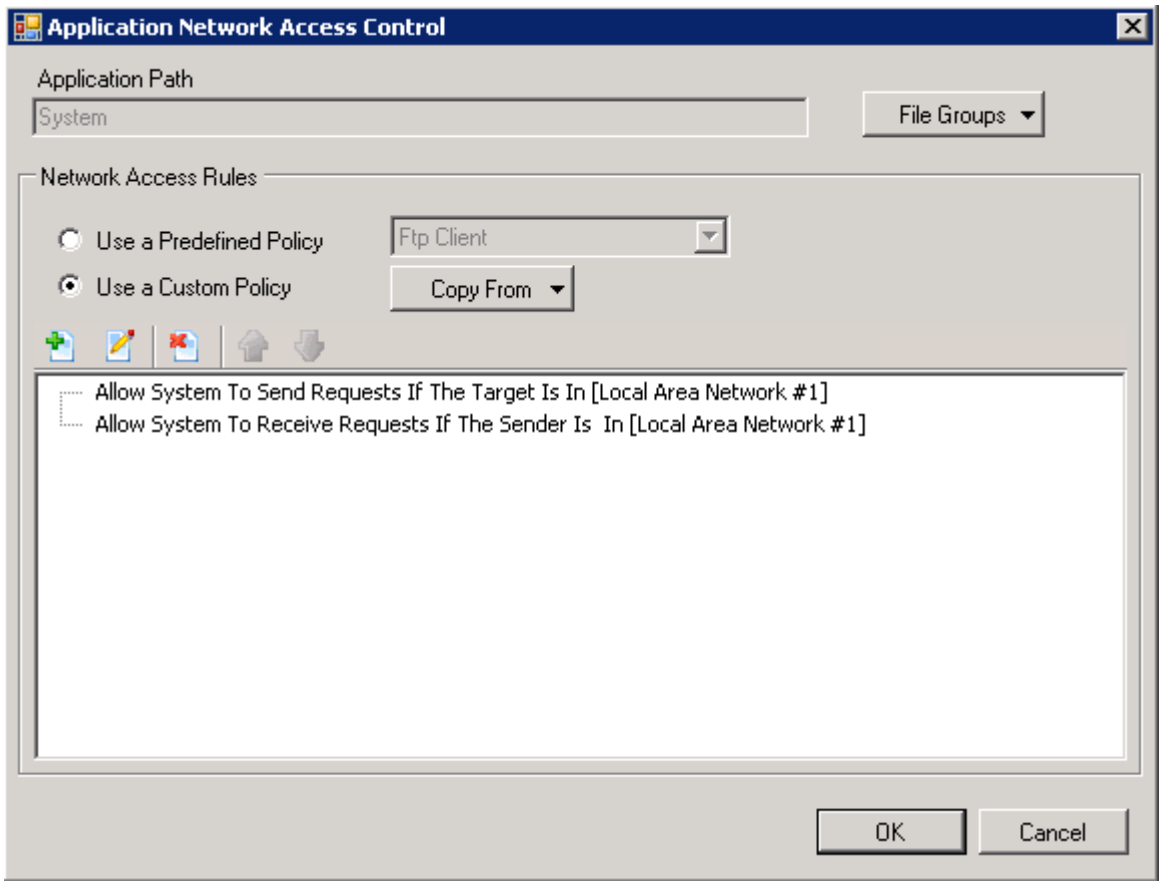
- Select the specific rule and click the icon to begin '**Adding and Editing a Network Control Rule**'

Note 1: Administrators can also re-prioritize policies or re-assign individual rules to another application's policy by dragging and dropping.

Note 2: Although each policy can be defined from the ground up by individually configuring its constituent rules, this practice would be time consuming if it had to be performed for every single program in the system. For this reason, Comodo Firewall contains a selection of predefined policies according to broad application category. For example, the policy 'Web Browser' can be applied to 'Internet Explorer', 'Firefox' and 'Opera' applications. Each predefined policy has been specifically designed by Comodo Firewall to optimize the security level of a certain type of application. Administrators can, of course, modify these predefined policies to suit their environment and requirements. For more details, see **Predefined Firewall Policies**.

Application Network Access Control interface

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



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

The priority of rules is re-ordered by simply dragging and dropping the rule in question. Alternatively, a rule can be re-prioritized by selecting it and clicking either the 'Move Up' or 'Move Down' button. To begin creating network policies, first read '**Overview of Policies and Rules**' then '**Creating and Modifying Network Policies**'

Creating and Modifying Network Policies

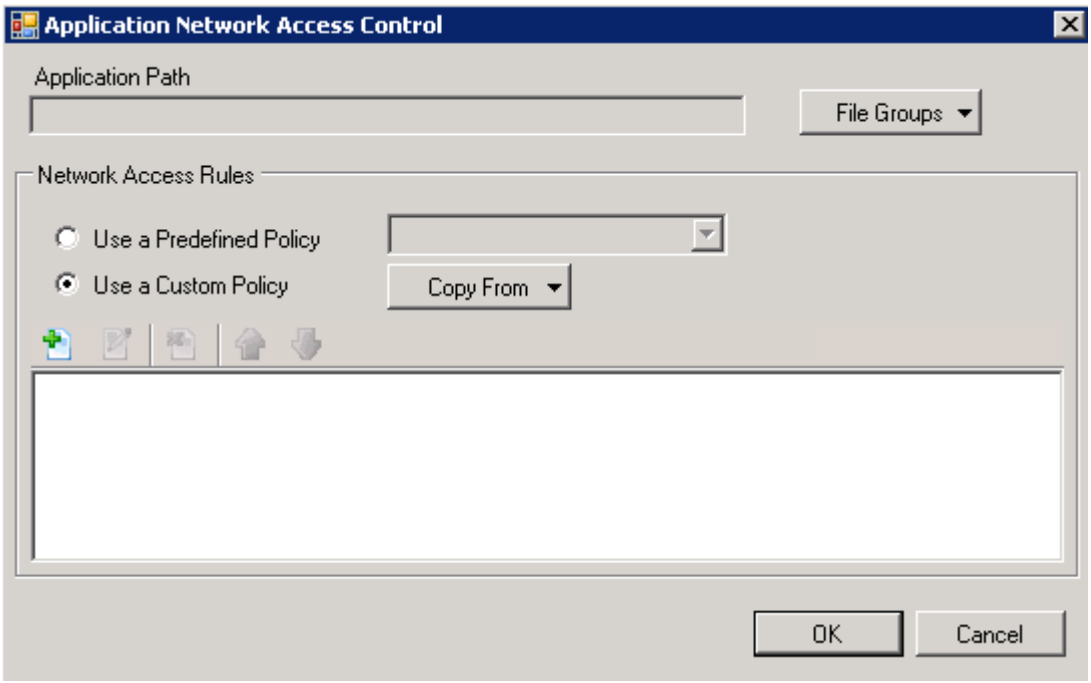
To begin defining an application's network policy, there are two basic steps:

(1) Select the application for which the policy is to be applied.

(2) Configure the rules for this application's policy.

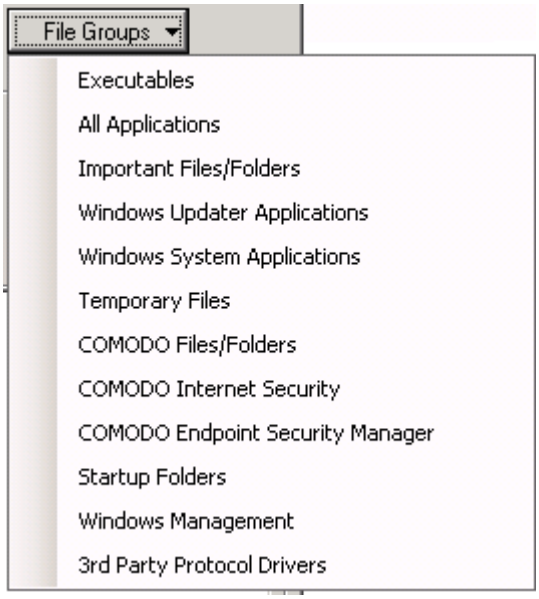
(1) Select the application for which the policy is to be applied

1. Click the  icon in the main **Application Rules tab**. This opens the **Application Network Access Control** dialog box shown below:



Note: As this is a new application, the 'Application Path' field is blank. While modifying an existing policy, this interface shows the individual rules for that application's policy.

2. Click **File Groups** button.



3. Select the required Application Path from the drop down.

Note 1: The File Group drop down displays a list of preset files or folders for which firewall policy is created. For example, selecting 'Executables' option creates a firewall policy for any file that attempts to connect to the Internet with the extensions .exe, .dll, .sys, .ocx, .bat, .pif, .scr, .cpl . Other such categories available include 'Windows System Applications' , 'Windows Updater Applications' , 'Start Up Folders' etc - each of which provide a fast and convenient way to apply a generic policy to important files and folders. To view the file types and folders that are affected by choosing one of these options, visit the Defense+ area of Comodo Internet Security by navigating to: Defense+ > My Protected Files

More details on Files and File Groupings is available in this help guide in the **My**

Protected Files and **My Blocked Files** sections.

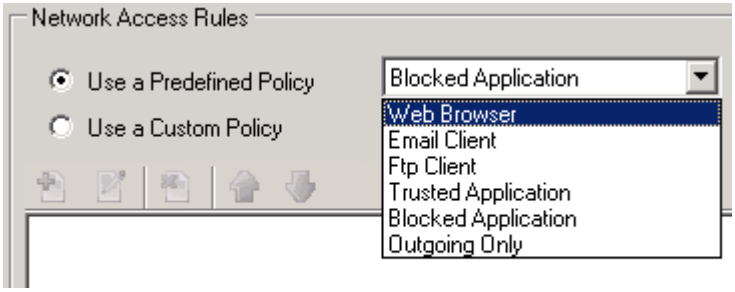
Note 2: To know how to create a new File Group and add a list of files to it, **Click here**.

(2) Configure the rules for this application's policy

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

(i) Use a Predefined Policy

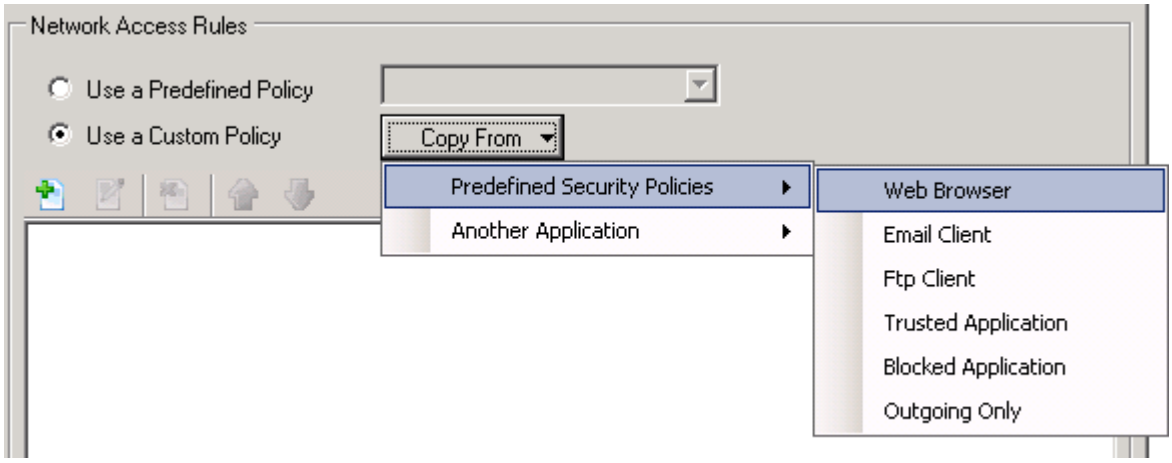
1. Select this option to quickly deploy an existing policy on to the target application.
2. Choose the policy from the drop-down menu. The name of the predefined policy is displayed in the **Treat As** column for the selected application in the **Application Rules** interface.



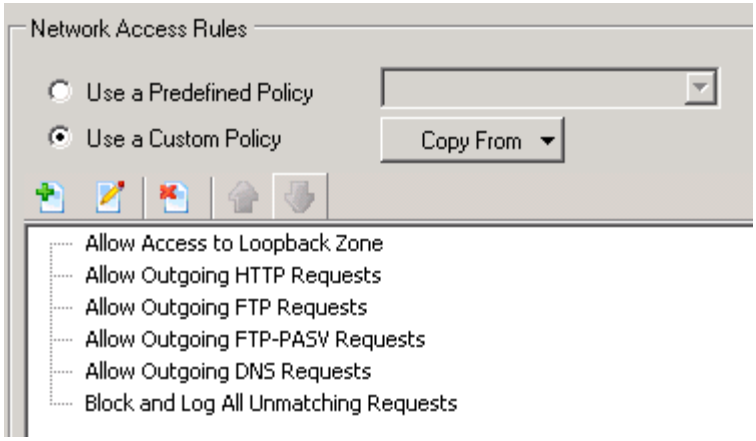
Note: It is not possible to modify Predefined Policies ***directly*** from this interface - they can only be modified and defined using the **Predefined Firewall Policies** interface. To add or modify rules for an application means creating a new custom policy and should be done using the more flexible **Use Custom Policy** option.

(ii) Use a Custom Policy: Designed for more experienced administrators.

1. Select this option to enable full control over the configuration of firewall policy and the parameters of each rule within that policy.
2. Click **Copy From** button. The various policy groups are displayed in the dropdown.



3. Click on the required policy group to display a list of policies associated with it in another dropdown.
4. Click the desired policy to populate the Network Access Rules section with the constituent rules of the predefined policy.



5. Select the rule and click the icon to **add or edit a Network Control Rule.**

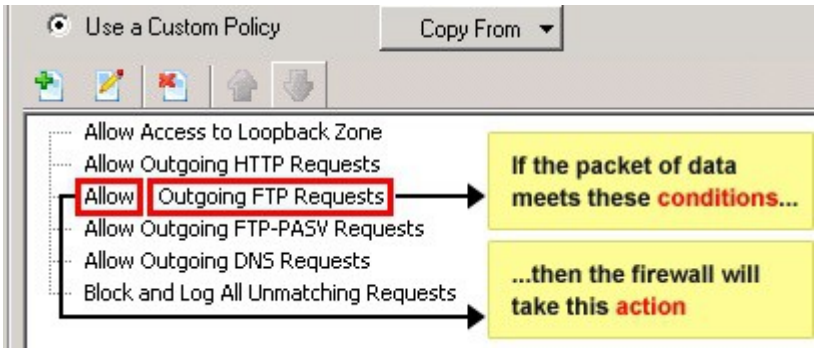
General Tips: To create a reusable policy for deployment on multiple applications, add a new **Predefined Firewall Policy** (or modify the existing ones accordingly), then use the **'Use Predefined Policy'** option in this section to roll it out.

To build a bespoke policy for maybe one or two specific applications, choose the **'Use a Custom Policy'** option and create a policy either from scratch by adding individual rules or by using one of the built-in policies as a starting point.

Understanding Network Control Rules

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

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



The actual **conditions** (attributes) seen* on a particular Network Control Rule are determined by the protocol chosen in **Adding and Editing a Network Control Rule**.

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

For 'ICMP', the rule has the form: **Action | Protocol | Direction | Source Address | Destination Address | ICMP Details**

For 'IP', the rule has the form: **Action | Protocol | Direction | Source Address | Destination Address | IP Details**

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

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

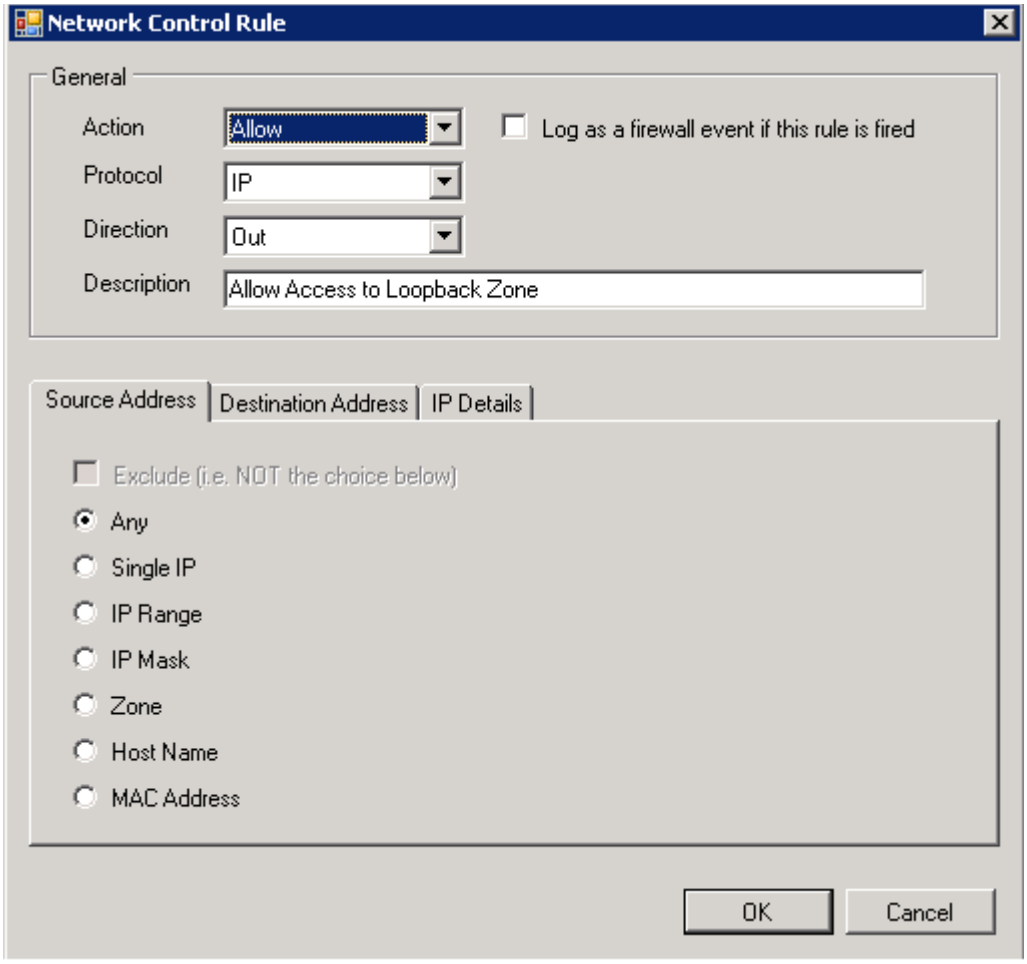
** If a descriptive name is defined while creating the rule, then that name is displayed here rather than it's full parameters. See the next section, 'Adding and Editing a Network Control Rule', for more details.*

*** Selecting 'Log as a firewall event if this rule is fired' option postfixes the action with "& Log". (e.g. Block & Log)*

Adding and Editing a Network Control Rule

The **Network Control Rule** Interface is used to configure the actions and conditions of an individual network control rule.

Note: Inexperienced firewall administrators are advised to gain some background knowledge by reading the sections '**Understanding Network Control Rules**' , '**Overview of Rules and Policies**' and '**Creating and Modifying Network Policies**'



General Settings

Action : Defines the action the firewall takes when the conditions of the rule are met. Options available via the drop down menu are **'Allow'**, **'Block'** or **'Ask'**.

Protocol: Allows the administrator to specify which protocol the data packet should use. Options available via the drop down menu are **'TCP'**, **'UDP'**, **'TCP or UDP'**, **'ICMP'** or **'IP'**.

Note: Based on the options selected in the Protocol field, the choices available in the tab structure on the lower half of the interface alters.

Direction: Allows the administrator to define which direction the packets should travel. Options available via the drop down menu are **'In'**, **'Out'** or **'In/Out'**

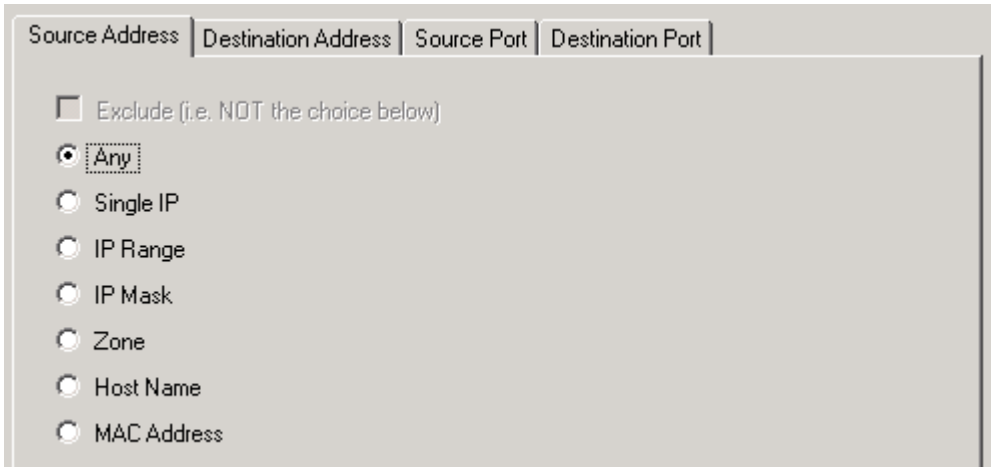
Log as a firewall event if this rule is fired: Selecting this option creates an entry in the **firewall event log viewer** whenever this rule is called into operation. (i.e. when ALL conditions have been met).

Description: A relative and descriptive name for the rule. Name a rule by it's intended purpose to understand easily, this is the name that is displayed to represent the rule instead of the full actions / conditions in the **main Application Rules Interface** and the **Application Network Access Control** interface.

TCP', 'UPD' or 'TCP or UDP' Protocol

If 'TCP', 'UPD' or 'TCP or UDP' is selected as the protocol for the network, then the source and destination IP addresses and ports receiving and sending the information must be defined.

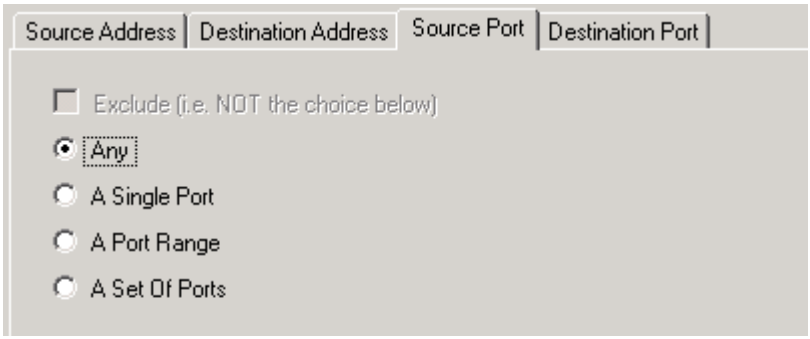
Source Address and Destination Address tab:



1. Choose any IP Address by selecting **Any** option. This menu defaults to an IP range of 0.0.0.0- 255.255.255.255 to allow connection from all IP addresses.
2. Choose a Single IP address by selecting **Single IP** option and enter the IP address in the **IP** text box, e.g., 192.168.200.113.
3. Choose an IP Range by selecting **IP Range** option and enter the the range of IP address in the **Start IP** and **End IP** fields respectively.
4. Choose IP Mask by selecting **IP Mask** option. IP networks can be divided into smaller networks called subnetworks (or subnets). An IP address / Mask is a subnet defined by IP address and mask of the network. Enter the **IP** address and **Mask** of the network in the respective fields.
5. Choose an entire network zone by selecting **Zone** option. This menu defaults to Local Area Network but new zones can also be defined by first creating a Zone through the **'My Network Zones'** interface.
6. Choose a named host by selecting a **Host Name** option, which denotes the IP address of the system being used.
7. Choose a MAC Address by selecting **MAC Address** option and entering the address in the **MAC Address** field.
8. Exclude (i.e. NOT the choice below)
9. Choosing the Exclude option performs the opposite of what is specified. For example, select **Allow** rule and check the **Exclude** box in the **Source IP** tab and enter values for the IP range, then that IP range is excluded.

Note: Create separate **Allow** rule for range of IP addresses that need not be used.

Source Port and Destination Port tab:



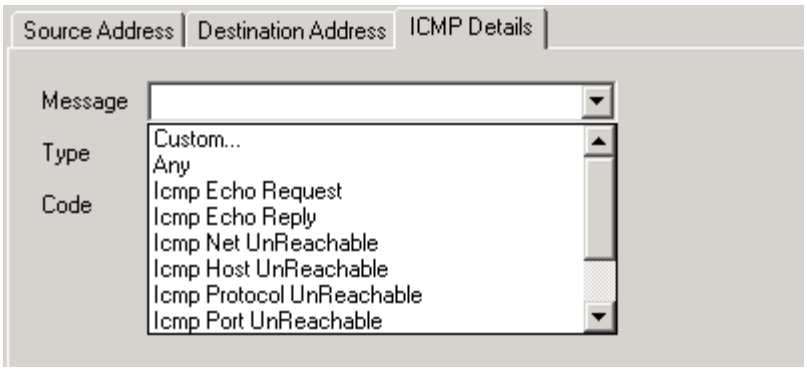
1. Choose any port number by selecting **Any** - set by default, 0- 65535.
2. Choose a Single Port number by selecting **A Single Port** option and selecting the single port numbers from the list.
3. Choose a Port Range by selecting **A Port Range** option and selecting the port numbers from the From and To list.
4. Choose a predefined port set by choosing **A Set of Ports** option. To create a port set please see the section **'My Port Sets'**.

ICMP Protocol

Selecting ICMP as the protocol in **General Settings**, shows a list of ICMP message type in the 'ICMP Details' tab alongside the **Source Address and Destination Address** tabs. The last two tabs are configured identically to the **explanation above.**

ICMP Details tab:

ICMP (Internet Control Message Protocol) packets contain error and control information which is used to announce network errors, network congestion, timeouts, and to assist in troubleshooting. It is used mainly for performing traces and pings. Pinging is frequently used to perform a quick test before attempting to initiate communications. It enables the administrator to create rules to allow / block specific types of ping requests. With Comodo Firewall administrators can create rules to allow / deny inbound ICMP packets that provide information and minimize security risk.



1. Enter the source / destination IP address. Source IP is the IP address from which the traffic originated and destination IP is the IP address of the computer that is receiving packets of information.
2. Specify the ICMP Message, Types and Codes. An ICMP message includes a Message that specifies the type, that is, the format of the ICMP message.
   - Selecting a particular ICMP message defaults to set its code and type as well.
   - Selecting the ICMP message type 'Custom' prompts to specify the code and type.

IP Protocol

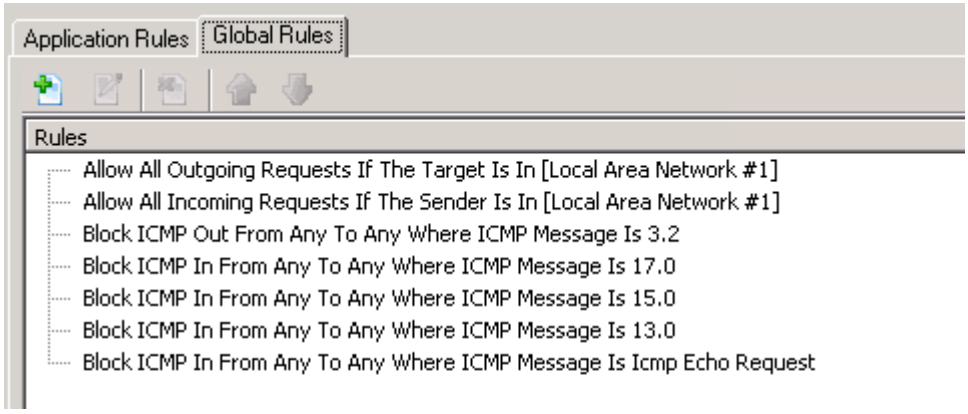
Selecting IP as the protocol in **General Settings**, shows a list of IP Protocols in the 'IP Details' tab alongside the **Source Address and Destination Address** tabs. The last two tabs are configured identically to the **explanation above**.

IP Details

1. Select the types of IP protocol that needs to be allowed. The IP protocols listed are ICMP (Internet Control Message Protocol), IGMP (Internet Group Management Protocol), GGP (Gateway-to-Gateway Protocol) , TCP (Transmission Control Protocol), UDP (User Datagram Protocol) and PUP (Parc Universal Packet).

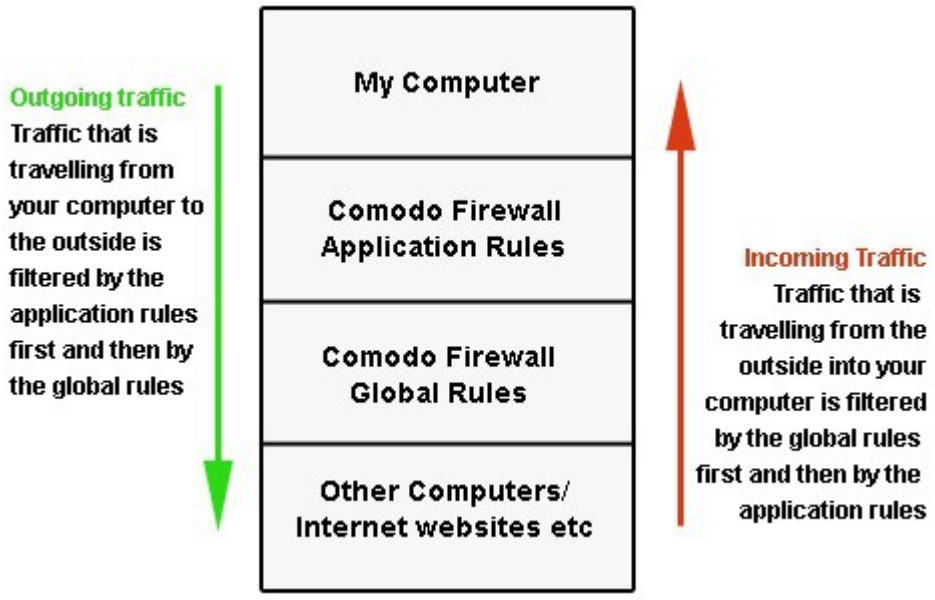
Global Rules

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



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

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



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

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

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

See **Application Network Access Control interface** for an introduction to the rule setting interface.

See **Understanding Network Control Rules** for an overview of the meaning, construction and importance of individual rules.

See **Adding and Editing a Network Control Rule** for an explanation of individual rule configuration.

4.1.2.2 Predefined Firewall Policies

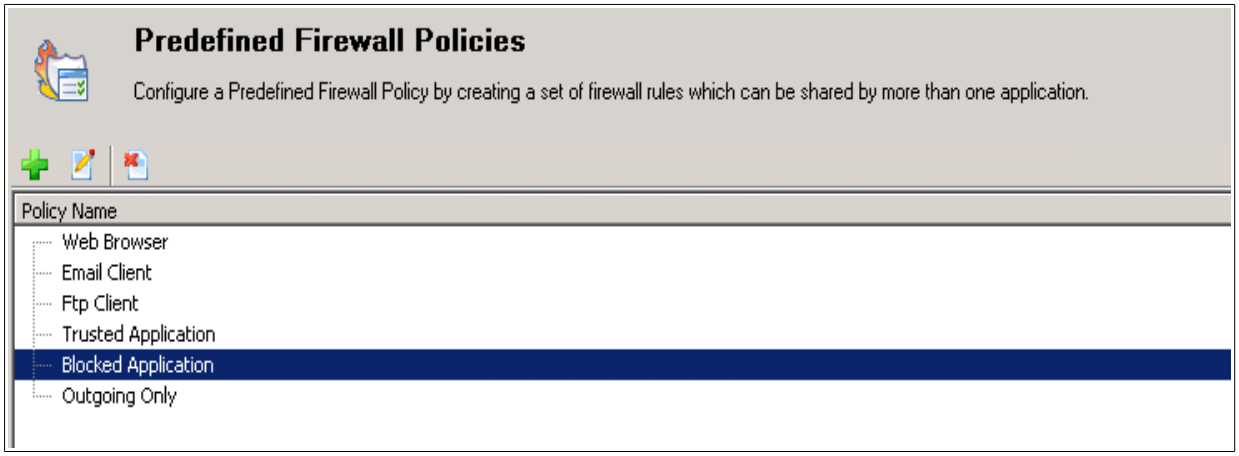
As the name suggests, a Predefined Firewall Policy is a set of one or more individual network control rules that have been saved and can be re-used and deployed on multiple applications.

Note: This section is for advanced and experienced administrators. Novice administrators are advised to first read the **Network Security Policy** section in this help guide.

Although each application's firewall policy *could* be defined from the ground up by individually configuring its constituent rules, this practice may prove time consuming if it had to be performed for every single program in the system. For this reason, Comodo Firewall contains a selection of predefined policies according to broad application category. For example, applying the

same policy such as 'Web Browser' to various application such as 'Internet Explorer', 'FireFox' and 'Opera'. Each predefined policy has been specifically designed by Comodo to optimize the security level of a certain type of application. Administrators can, of course, modify these predefined policies to suit their environment and requirements. For example, the name 'Web Browsers' can be retained but the parameters of its rules can be redefined, if needed.

- Click on **Predefined Firewall Policies** in Firewall > Advanced Tasks to open the 'Predefined Firewall Policies' interface.



To view or edit an existing predefined policy

- Double click on the Policy Name in the list

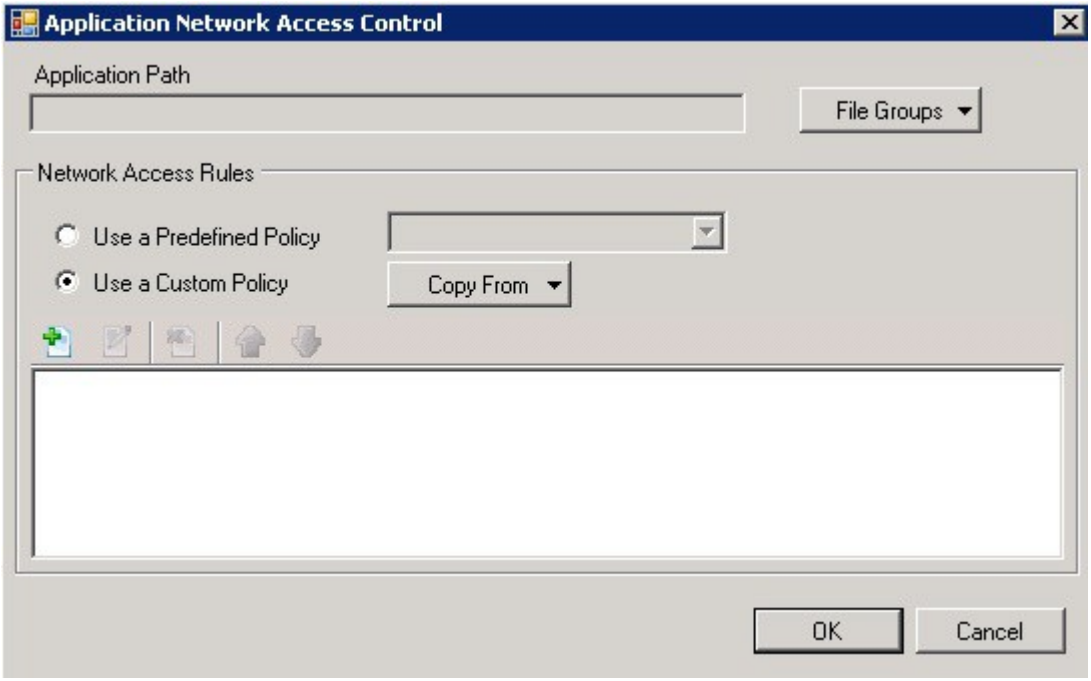
  (OR)

- Select the Policy Name in the list and click the  icon

Details of the process from this point on can be found **here**

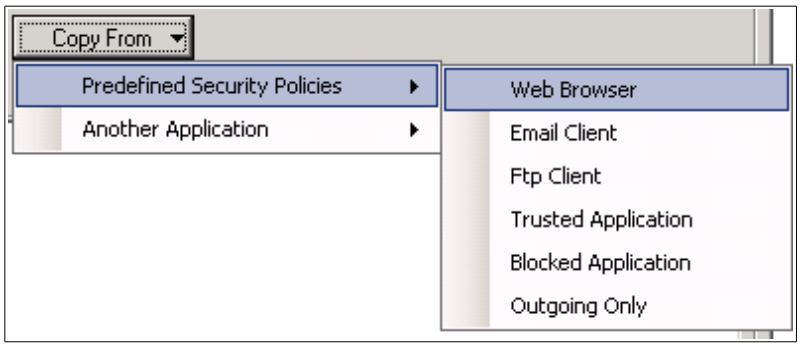
To add a new predefined policy

1. Click the  icon. This launches the policy creation dialog shown below.



As this is a new application, the 'Application Path' field is blank. Choose a name that accurately describes the category / type of application for which the policy is defined. Next, add and configure the individual rules for this policy. See '**Adding and Editing a Network Control Rule**' for more advice on this.

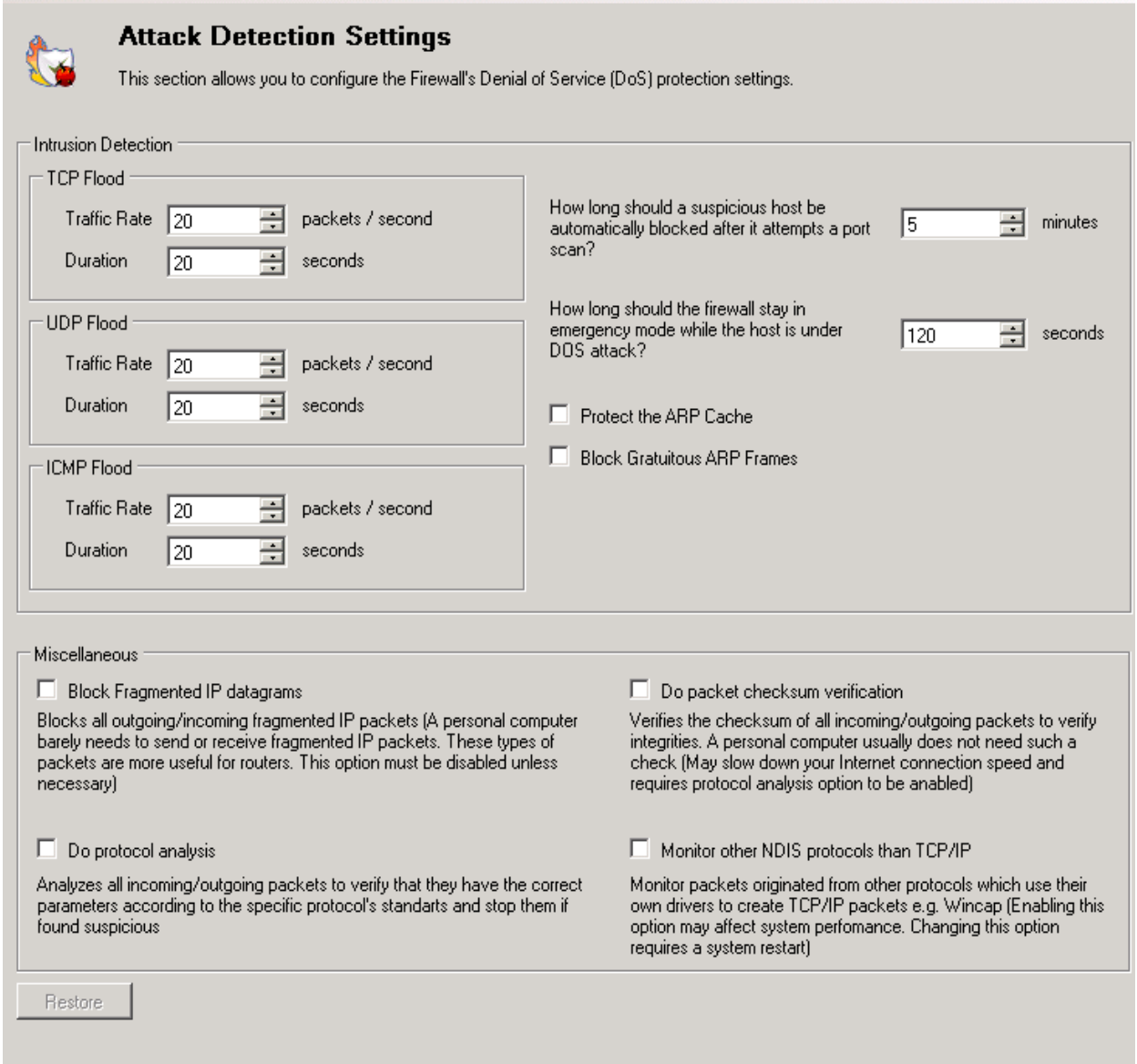
Once created, this policy is quickly called as a 'Predefined Policy' when **creating or modifying a network policy**.



4.1.2.3 Attack Detection Settings

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

- Click on **Attack Detection Settings** in Firewall > Advanced Tasks to open the 'Attack Detection Settings' interface.



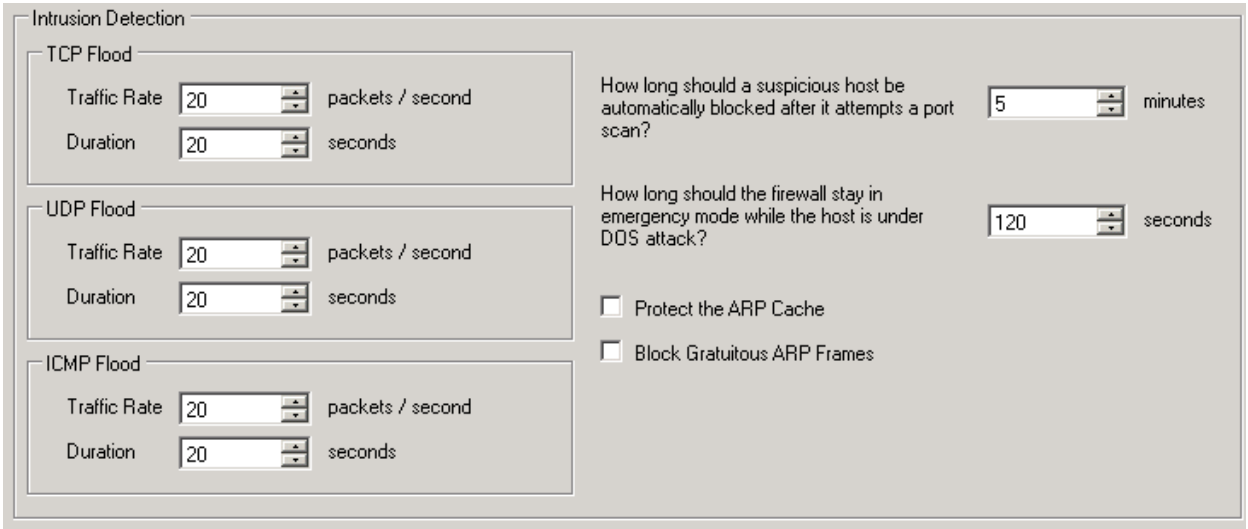
The Attack Detection Settings area allows to configure the protection parameters in two sections:

- **Intrusion Detection** tab
- **Miscellaneous** tab

Intrusion Detection tab

Options - Intrusion Detection section	
Option	**Description**
TCP Flood / UDP Flood / ICMP Flood	Flood attacks happen when thousands of packets of data are sent from a spoofed IP source address to a target machine. The target machine automatically sends back a response to these requests (a SYN packet) and waits for an acknowledgment (an ACK packet). But, because they were "sent" from a spoofed IP address, the target machine never receives any responses / acknowledgment packets. This results in a backlog of unanswered requests that begins to fill up the target connection table. When the connection table is full, the target machine refuses to accept any new connections - which means the computer is no longer able to connect to the Internet, send email, use FTP services etc. When this happens multiple times from multiple sources it floods the target machine, which has a limit of unacknowledged responses it can handle, and may cause it to crash. By default, Comodo Firewall is configured to accept traffic using TCP, UDP and ICMP protocols at a maximum rate of packets per second for a set duration of time. The defaults are for all three protocols are set at 20 packets per second for a continuous duration of 20 seconds. The number of packets per second and the maximum duration that the firewall should accept packets at this rate can be reconfigured to the administrator's preference. If these thresholds exceed, a DOS attack is detected and the Firewall goes into emergency mode. The firewall stays in emergency mode for the duration set by administrator. By default this is set at 120 seconds. Administrators can alter this time length to their own preference by configuring **How long should the firewall stay in emergency mode while the host is under DOS attack**? In emergency mode, all inbound traffic is blocked except those previously established and active connections. However, all outbound traffic is still allowed.
How long should a suspicious host be automatically blocked after it attempts a port scan?	Port scanning, a favorite approach of computer cracker, gives the assailant an idea where to probe for weaknesses. Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed for weakness. Comodo Firewall detects the most common forms of port scans, alerting the administrator and temporarily blocking and banning the IP address of the scanner, ensuring that they are "cut off" before they can discover any useful information about the system. Administrators have the option to configure how long to block incoming traffic from a host suspected of perpetrating a port scan. If a port scan is detected, the Firewall identifies the host scanning the system as suspicious and automatically blocks it for a set period of time - by default 5 minutes. During this time, no traffic is accepted from the host. During these 5 minutes, the suspicious host cannot access the administrator's system but the administrator's system can access it.
How long should the firewall stay in emergency mode whilst the host is under DOS attack?	When a DOS attack is detected, the Firewall goes into emergency mode for a fixed period of time - set by default to 120 seconds. Administrator can configure the length of time to their own preferences.
Protect the ARP Cache	Checking this option makes Comodo Firewall to start performing stateful inspection of ARP (Address Resolution Protocol) connections. This blocks spoof ARP requests and protect the computer from ARP cache poisoning attacks. The ARP Cache (or ARP Table) is a record of IP addresses stored in the computer that is used to map IP addresses to MAC addresses. Stateful inspection involves the analysis of data within the lowest levels of the protocol stack and comparing the current session to previous ones in order to detect suspicious activity.

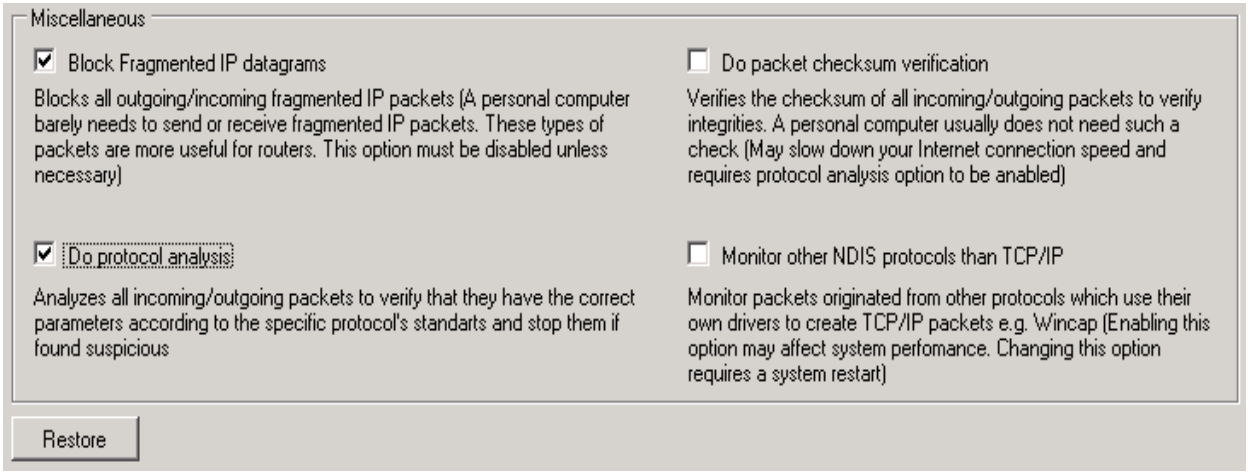
Options - Intrusion Detection section	
	Background - Every device on a network has two addresses: a MAC (Media Access Control) address and an IP (Internet Protocol) address. The MAC address is the address of the physical network interface card inside the device, and never changes for the life of the device (in other words, the network card inside the PC has a hard coded MAC address that it keeps even if installed it in a different machine.) On the other hand, the IP address can change if the machine moves to another part of the network or the network uses DHCP to assign dynamic IP addresses. In order to correctly route a packet of data from a host to the destination network card it is essential to maintain a record of the correlation between a device's IP address and it's MAC address. The Address Resolution Protocol performs this function by matching an IP address to its appropriate MAC address (and vice versa). The ARP cache is a record of all the IP and MAC addresses that the computer has matched together. Hackers can potentially alter a computer's ARP cache of matching IP / MAC address pairs to launch a variety of attacks including, Denial of Service attacks, Man in the Middle attacks and MAC address flooding and ARP request spoofing. It should be noted, that a successful ARP attack is almost always dependent on the hacker having physical access to the network or direct control of a machine in the network - therefore this setting is of more relevance to network administrators.
Block Gratuitous ARP Frames	A Gratuitous ARP frame is an ARP Reply that is broadcast to all machines in a network and is not in response to any ARP Request. When an ARP Reply is broadcast, all hosts are required to update their local ARP caches, whether or not the ARP Reply was in response to an ARP Request they had issued. Gratuitous ARP frames are important as they update the machine's ARP cache whenever there is a change to another machine on the network (for example, if a network card is replaced in a machine on the network, then a gratuitous ARP frame informs the administrator's machine of this change and request to update the ARP cache so that data can be correctly routed). Enabling this setting blocks such requests - protecting the ARP cache from potentially malicious updates.



1. To reconfigure the Traffic Rate and Duration of TCP Flood, UDP Flood and ICMP Flood, if necessary, use the corresponding up / down buttons.
2. To block a suspicious host for a particular duration use the up / down button to set the minutes in the 'How long should a suspicious host be automatically blocked after it attempts a port scan?' field.
3. To set firewall duration during DOS attack, use the up / down button to set the seconds in the 'How long should the firewall stay in emergency mode whilst the host is under DOS attack?' field.
4. Select the respective check boxes to 'Protect the ARP Cache' and to 'Block Gratuitous ARP Frames'.

Miscellaneous tab

Checkbox Options - Miscellaneous section	
Option	**Description**
Block fragmented IP Datagrams	When a connection is opened between two computers, they must agree on a Mass Transmission Unit (MTU). IP Datagram fragmentation occurs when data passes through a router with an MTU less than the MTU being used i.e when a datagram is larger than the MTU of the network over which it must be sent, it is divided into smaller 'fragments' which are each sent separately. Fragmented IP packets can create threats similar to a DOS attack. Moreover, these fragmentation can double the amount of time it takes to send a single packet and slow down the download time. Comodo Firewall is set by default to block fragmented IP datagrams i.e the option Block Fragmented IP datagrams is checked by default.
Do Protocol Analysis	Protocol Analysis is key to the detection of fake packets used in DOS attacks. Checking this option means Comodo Firewall checks every packet conforms to that protocols standards. If not, then the packets are blocked
Do Packet Checksum Verification	Every packet of data sent to a machine has a signature attached. With this option enabled, Comodo Firewall recalculates the checksum of the incoming packet and compare this against the checksum stated in the signature. If the two do not match then the packet has been altered since transmission and Comodo Firewall blocks it. Although this feature has security benefits it is also very resource intensive and the Internet connection speed may take a large hit if checksum verification is performed on each packet. This feature is intended for use by advanced administrators and Comodo advise not to enable this feature.
Monitor other NDIS protocols than TCP/IP	This forces Comodo Firewall to capture the packets belonging to any other protocol diver than TCP/IP. Trojans *can potentially* use their own protocol driver to send / receive packets. This option is useful to catch such attempts. This option is disabled by default because it can reduce system performance and may be incompatible with some protocol drivers.



1. Select the checkboxes of the appropriate option.
2. Click the Restore button to reset all the values if necessary.

Note: The Restore button is enabled only if there are any changes made in the existing settings.

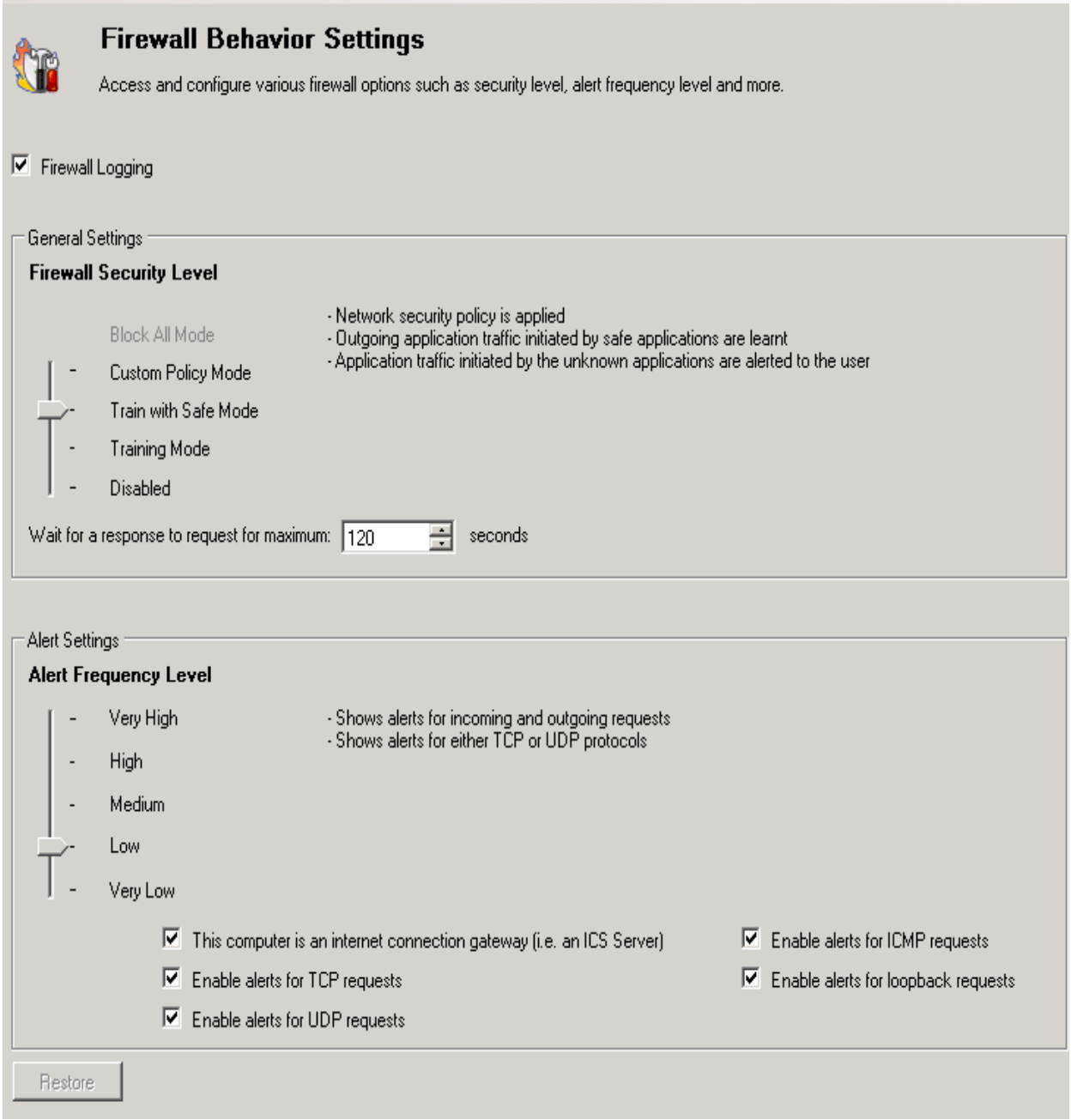
4.1.2.4 Firewall Behavior Settings

Firewall Behavior Settings allows quick configuration of security of a computer and the frequency of alerts that are generated.

- Click on **Firewall Behavior Settings** in Firewall > Advanced Task to open the 'Firewall Behavior Settings' interface.

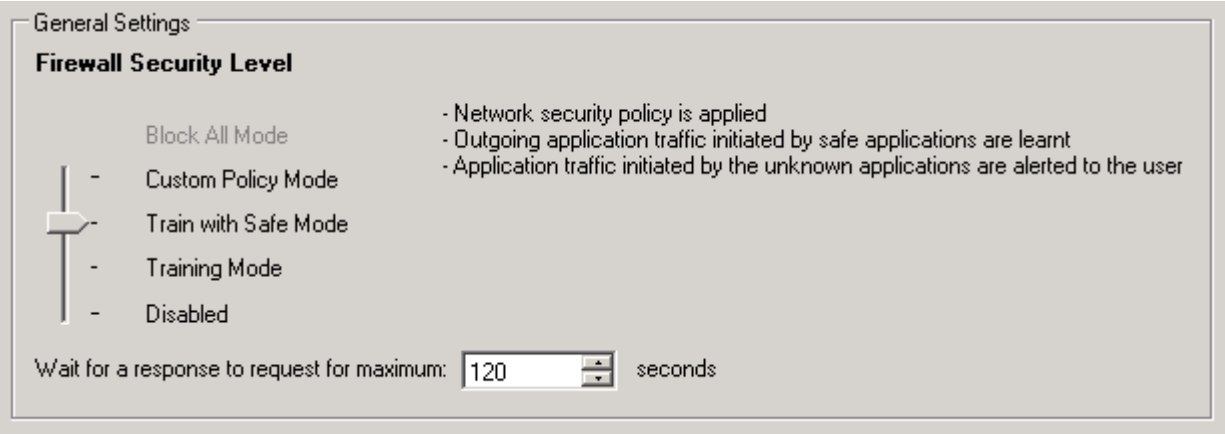
These settings are divided into two sections.

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



General Settings section

Comodo Firewall allows customization of firewall security by using the Firewall Security Level slider to change preset security levels.



Slider Options:

Slider Options - General Settings	
Option	**Description**
Block All Mode	The firewall blocks all traffic in and out of a computer regardless of any predefined configuration and rules. The firewall does not attempt to learn the behavior of any applications and does not automatically create traffic rules for any applications. Choosing this option effectively prevents the computer from accessing any networks, including the Internet. **Note**: This option is disabled.
Custom Policy Mode	The firewall applies ONLY the custom security configurations and **network traffic policies** specified by the administrator. New administrators may want to think of this as the 'Do Not Learn' setting because the firewall does not attempt to learn the behavior of any applications. Nor does it automatically create network traffic rules for those applications. Alerts are received every time there is a connection attempt by an application - even for applications on the Comodo Safe list (unless rules and policies are specified that instruct the firewall to trust the application's connection attempt). If any application tries to make a connection to the outside, the firewall audits all the loaded components and checks each against the list of components already allowed or blocked. If a component is found to be blocked, the entire application is denied Internet access and an alert is generated. This setting is advised for experienced firewall administrators who wish to maximize the visibility and control over traffic in and out of their computer.
Safe Mode	While filtering network traffic, the firewall automatically creates rules that allow all traffic for the components of applications certified as 'Safe' by Comodo. For non-certified new applications, an alert is received whenever that application attempts to access the network. To grant the application internet access, choose 'Treat this application as a Trusted Application' at the alert. This deploys the **predefined firewall policy** 'Trusted Application' onto the application. 'Train with Safe Mode' is the recommended setting for most administrators - combining the highest levels of security with an easy-to-manage number of connection alerts.
Training Mode	The firewall monitors network traffic and create automatic allow rules for all new applications until the security level is adjusted. No alerts are received in 'Training Mode' mode. Before choosing 'Training Mode' setting, be 100% sure that all applications installed on the computer are assigned the **correct network access rights**. ***Tip***: Use this setting temporarily while playing an online game for the first time. This suppresses all alerts while the firewall learns the components of the game that need Internet access and automatically create 'allow' rules for them. Afterward it can be switched back to the previous mode.
Disabled	Disables the firewall and makes it inactive. All incoming and outgoing connections are allowed irrespective of

Slider Options - General Settings	
	the restrictions set by the administrator. Comodo strongly advise against this setting unless the system is not currently connected to any local or wireless networks.

1. Move the slider to select the required Firewall Security Level. The description corresponding to the selected option is displayed in the right hand side of the options.
2. Select the 'Wait for a response to request for maximum' value by using the  up / down arrow buttons. The time entered here determines how long the application waits for a response from the CESM Central Service (see the CESM Admin Guide - Request Monitor section for more details).

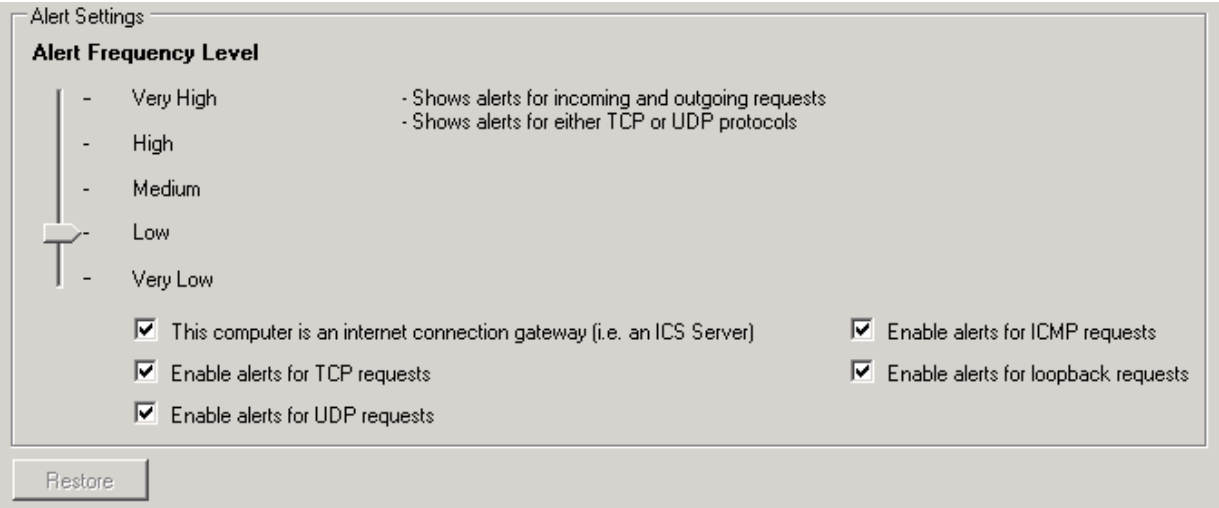
Alert Settings tab

Administrators can configure the amount of alerts that Comodo Firewall generates, using the slider in this section. Raising or lowering the slider changes the amount of alerts accordingly. It should be noted that this does not affect the security, which is determined by the rules being configured (for example, in '**Network Security Policy**'). For the majority of administrators, the default setting of 'Low' is the perfect level - ensuring that connection attempts are informed and suspicious behaviors whilst not overwhelming with alert messages.

The Alert Frequency settings refer only to connection attempts by applications or from IP addresses that are not yet declared as trustable. For example, a very high alert frequency level can be specified, but does not receive any alerts at all if the application that is making the connection attempt is marked as trustable.

Slider Options - Alert Settings	
Option	**Description**
Very High	The firewall shows separate alerts for outgoing and incoming connection requests for both TCP and UDP protocols on specific ports and for specific IP addresses, for an application. This setting provides the highest degree of visibility to inbound and outbound connection attempts but leads to a proliferation of firewall alerts. For example, using a browser to connect to an Internet home-page may generate as many as 5 separate alerts for an outgoing TCP connection alone.
High	The firewall shows separate alerts for outgoing and incoming connection requests for both TCP and UDP protocols on specific ports for an application.
Medium	The firewall shows alerts for outgoing and incoming connection requests for both TCP and UDP protocols for an application.
Low	The firewall shows alerts for outgoing and incoming connection requests for an application. This is the setting recommended by Comodo and is suitable for majority of administrators.
Very Low	The firewall shows only one alert for an application.
Checkbox Options – Alert Settings	
This computer is an Internet connection gateway (i.e. an ICS server)	An Internet Connection Sharing Server (ICS) is a computer that shares its connection to the Internet with other computers that are connected to it by LAN. i.e. the other computers access the Internet through this computer. Designating a computer as an ICS server can be useful in some corporate and home

Slider Options - Alert Settings	
	environments that have more than one computer but which have only one connection to the Internet. For example, there might be 2 computers in a place but only one connection. Setting one as an ICS server allows both of them to access the Internet. Leave this box unchecked if no other systems are connected the computer via Local Area Network to share the connection. Check this option if this computer has been configured as an Internet Connection Sharing server through which other computers connect to the Internet. **Note:** If the main computer is indeed an ICS server but this option is left unchecked then there is likely to be an increase in Firewall alerts. Selecting this checkbox does not decrease the security but tells the firewall to handle ICS requests too. So it just activates some additional functionality and helps reduce the number of alerts.
Enable alerts for TCP requests / Enable alerts for UDP requests / Enable alerts for ICMP requests / Enable Alerts for loopback requests	In conjunction with the slider, these checkboxes allow to fine-tune the number of alerts seen according to protocol.



1. Move the slider to select the required Alert Frequency Level. The description corresponding to the selected option is displayed in the right hand side of the options.
2. Select the checkboxes of the appropriate option.
3. Click the Restore button to reset all the values if necessary.

Note: The Restore button is enabled only if there are any changes made in the existing settings.

4.2. Defense+ Overview

The Defense+ component of Comodo Internet Security (hereafter known simply as Defense+) is a host intrusion prevention system that constantly monitors the activities of all executable files on a PC. With Defense+ activated, the administrator is warned EVERY time an unknown executable application (.exe, .dll, .sys, .bat etc) attempts to run. The only executables that are allowed to run are the ones the administrator gives permission to.

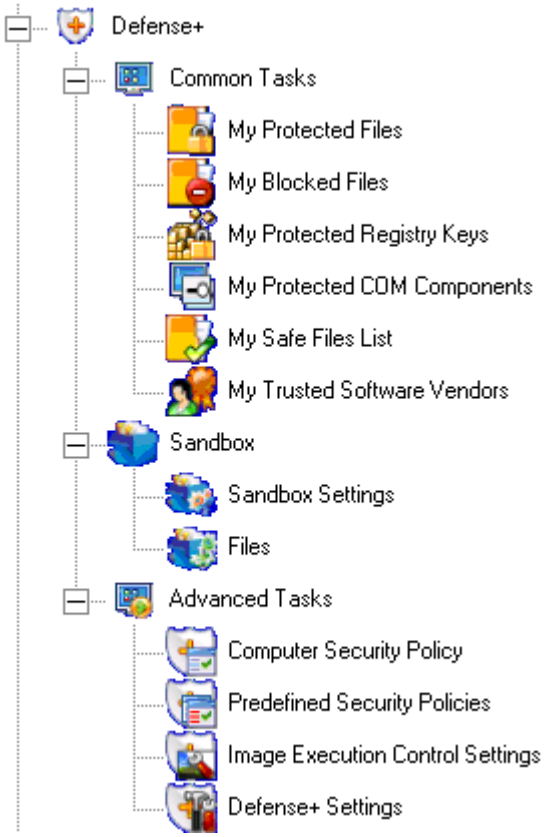
The Sandbox functionality of Defense+ allows you to run suspicious and unknown executables in an isolated environment to safeguard your system from the adverse effects of those executables. This is useful for software testers and users interested in testing out the new software available over Internet. For more details refer to **Sandbox Operations**.

Defense+ also protects against data theft, computer crashes and system damage by preventing most types of buffer overflow attacks. This type of attack occurs when a malicious program or script deliberately sends more data to its memory buffer than that the buffer can handle. It is at this point that a successful attack can create a back door to the system through which a hacker can gain access. The goal of most attacks is to install malware onto the compromised PC whereby the hacker can reformat the hard drive, steal sensitive information, or even install programs that transform the machine into a Zombie PC. For more details refer **Image Execution Control Settings**.

Defense+ boasts a highly configurable security rules interface and prevents possible attacks from root-kits, inter-process memory injections, key-loggers and more. It blocks Viruses, Trojans and Spyware before they can ever get installed on a system and prevents unauthorized modification of critical operating system files and registry entries.

The Defense+ center allows to quickly and easily configure all aspects of Defense+ and is divided into two sections: **Common Tasks,** Sandbox and **Advanced Tasks**.

Defense+ center can be accessed at all times by clicking on the Defense+ Shield button 



4.2.1. Common Tasks

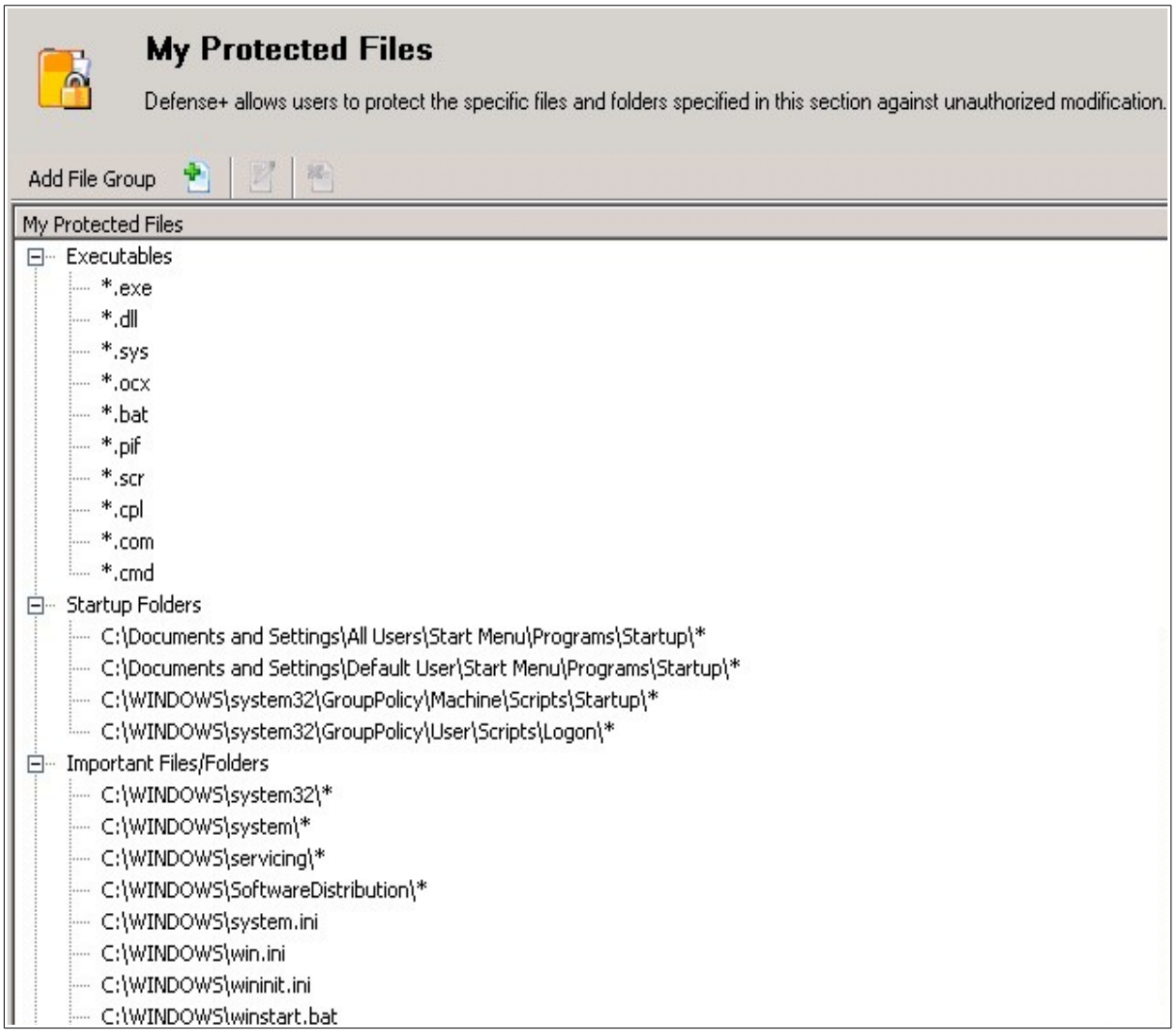
Click the links below to see detailed explanations of each area in this section.

- **My Protected Files**
- **My Blocked Files**
- **My Protected Registry Keys**
- **My Protected COM Interfaces**
- **My Safe Files List**
- **My Trusted Software Vendors**

4.2.1.1. My Protected Files

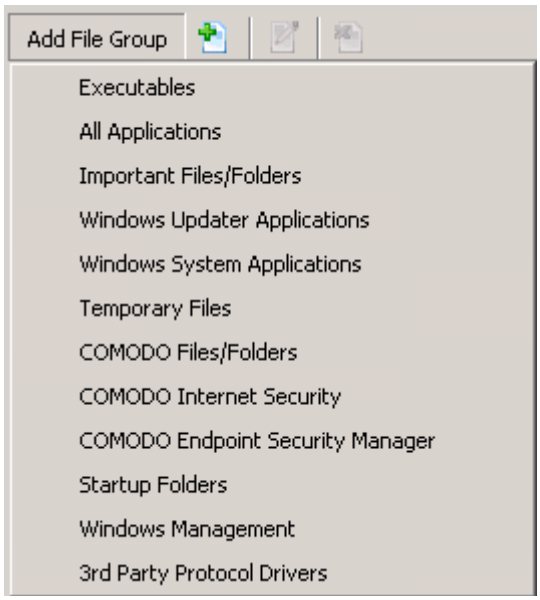
My Protected Files setting helps protect specific files and folders against unauthorized modification. Protecting files prevents modification by malicious programs such as virus, Trojans and spyware. It is also useful for safeguarding very valuable files (spreadsheets, databases, documents) by denying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

- Click on **My Protected Files** in Defense+ > Common Tasks to open 'My Protected Files' interface.



To add an existing File Group

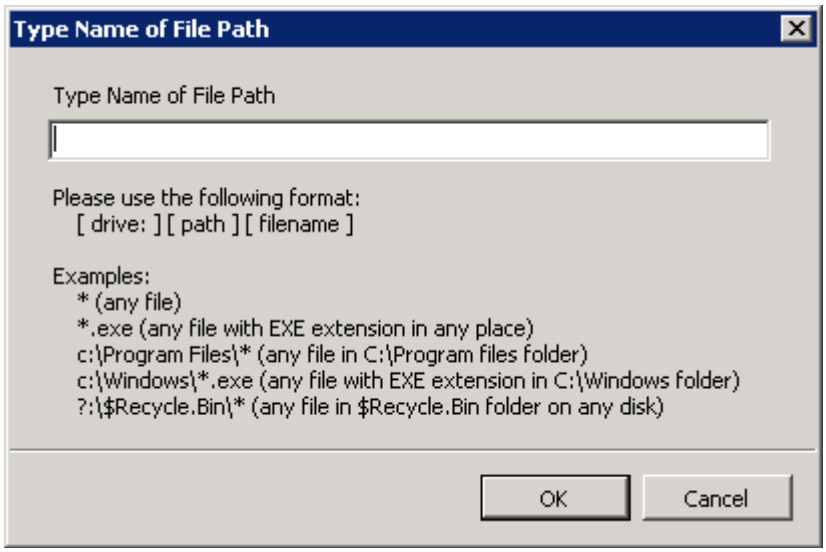
1. Click the Add File Group button to display the list of existing file groups. **Click here** for a description of the choices available when selecting a file.



2. Select the required File Group from the list. The selected File Group is displayed in the 'My Protected Files' main list.

To add a File to a file group

1. Select the required file group and click the icon. The 'Type Name of File Path' dialog box is displayed.

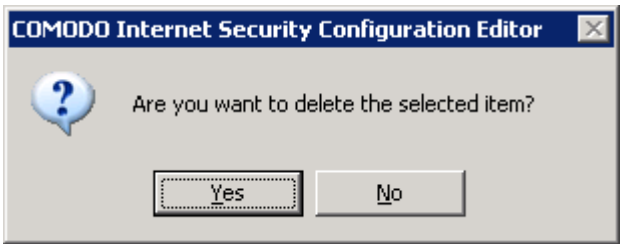


2. Type the name of the file path in the format specified in the dialog box.
3. Click **OK** to confirm. The name of the added file path is displayed in the main list under the selected file group.

Note: To know how to create a new File Group and add a list of files to it, **Click here**.

To delete a File Group

1. Select the required File Group and click the icon. The following confirmation dialog box is displayed.



2. Click **Yes** to delete the selected item.

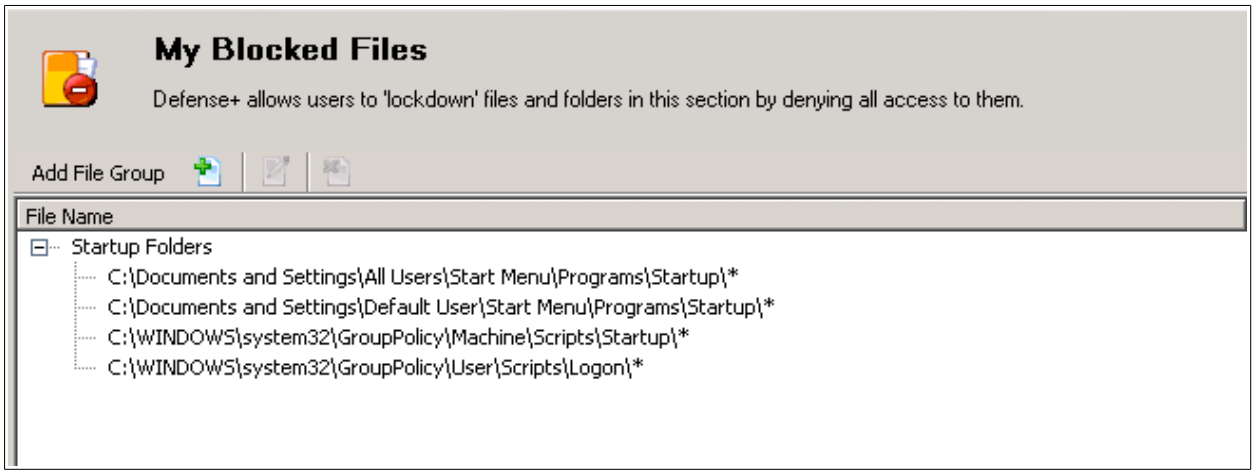
Note 1: Only File Groups can be deleted in this interface. It is not possible to delete any Files under a file group in this interface.

Note 2: This area is for adding file groups only. It is not possible to to modify the security policy of any applications or files from here. To do that, use the **Computer Security Policy** interface or the **Predefined Security Policy** Interface.

4.2.1.2. My Blocked Files

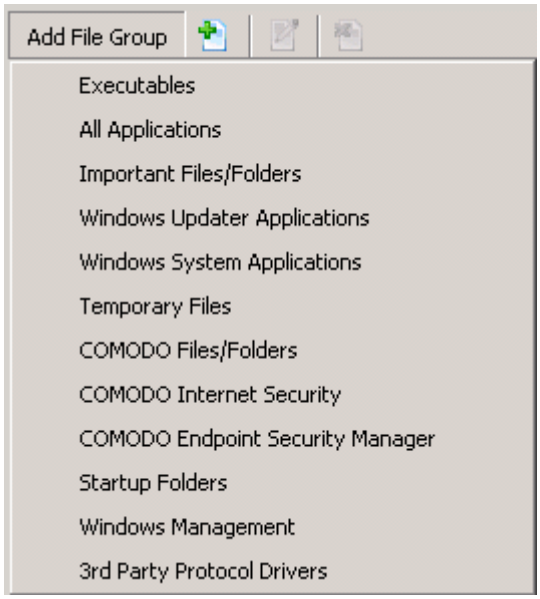
Defense+ allows to lock-down files and folders by completely denying all access rights to them from other processes or machines **-** effectively cutting it off from the rest of the system. If the file being blocked is an executable, then nothing else is able to run that program. Unlike files that are placed in 'My Protected Files', administrators cannot selectively allow any process access to a blocked file.

- Click on **My Blocked Files** in Defense+ > Common Tasks > to open 'My Blocked Files' interface.



To add an existing File Group or process

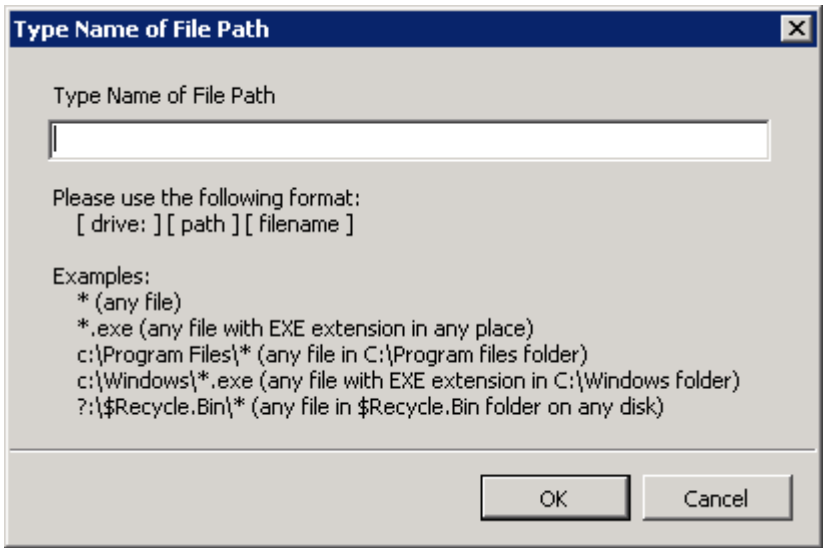
1. Click the Add File Group button to display the list of existing groups. **Click here** for a description of the choices available when selecting a file.



2. Select the required File Group from the list. The selected File Group is displayed in the 'My Blocked Files' main list.

To add a File to a file group

1. Select the required file group and click the icon. The 'Type Name of File Path' dialog box is displayed.

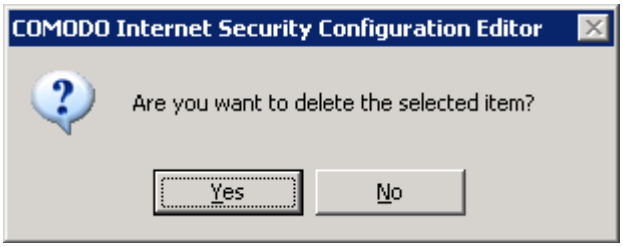


2. Type the name of the file path in the format specified in the dialog box.
3. Click **OK** to confirm. The name of the added file path is displayed in the main list under the selected file group.

Note: To know how to create a new File Group and add a list of files to it, **Click here**.

To delete a File Group

1. Select the required File Group and click the  icon. The following confirmation dialog box is displayed.



2. Click **Yes** to delete the selected item.

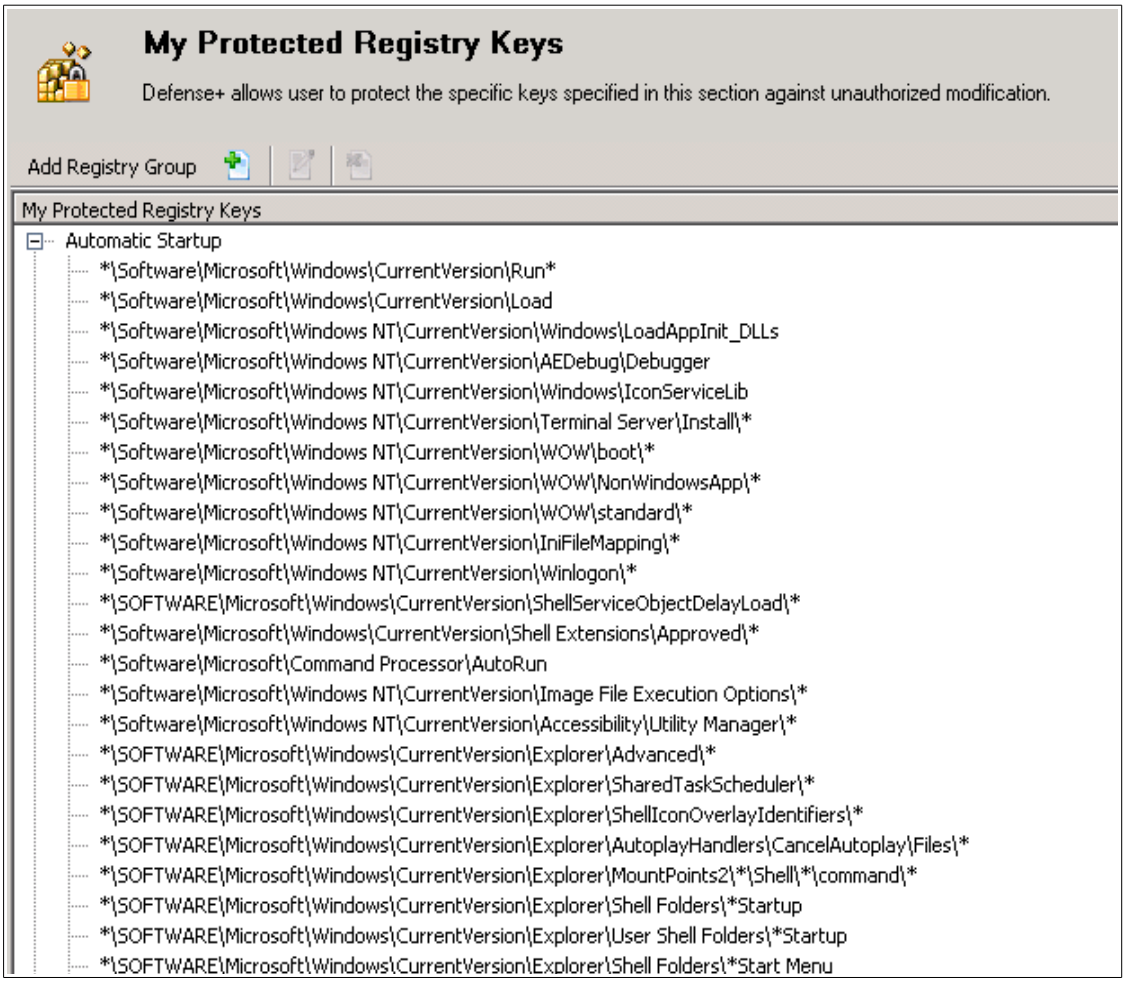
Note 1: Only File Groups can be deleted in this interface. It is not possible to delete any Files under a file group in this interface.

Note 2: This area is for adding file groups only. It is not possible to to modify the security policy of any applications or files from here. To do that, use the **Computer Security Policy** interface or the **Predefined Security Policy** Interface.

4.2.1.3. My Protected Registry Keys

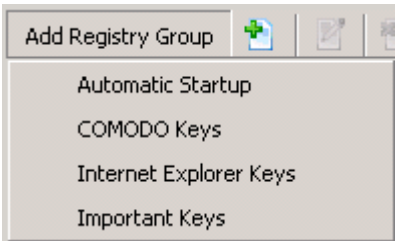
Comodo Internet Security automatically protects system critical registry keys against modification. Irreversible damage can be caused to a system if important registry keys are corrupted or modified in any way . It is essential that a system's registry keys are protected against attack.

- Click on **My Protected Registry Keys** in Defense+ > Common Tasks to open 'My Protected Registry Keys' interface.



To add an existing Registry Group

1. Click the Add Registry Group button to display the list of existing groups.

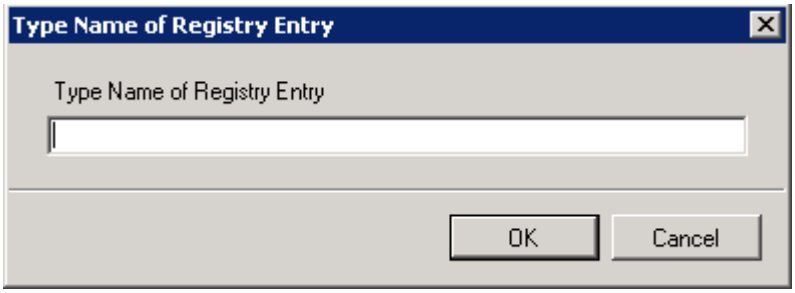


Note: The 'Add Registry Groups' option allows to batch select and import predefined groups of important registry keys. Comodo Internet Security provides a default selection of 'Automatic Startup' (keys), 'Comodo Keys', 'Internet Explorer Keys' and 'Important Keys'.

1. Select the required Registry Group from the list. The selected Registry Group is displayed in the 'My Protected Registry Keys' main list.

To add a Registry Key to a Registry group

1. Select the required Registry group and click the icon. The 'Type Name of Registry Entry' dialog box is displayed.

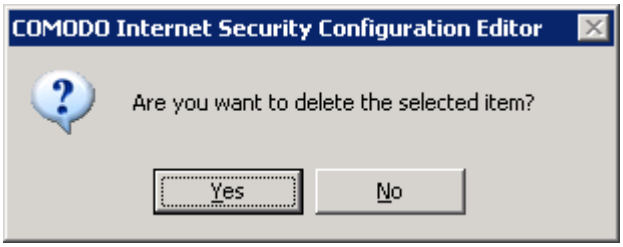


2. Type the name of the Registry Entry.
3. Click **OK** to confirm. The name of the new registry key is displayed in the main list under the selected registry group.

Note: To know how to create a new File Group and add a list of files to it, **Click here**.

To delete a Registry Group

1. Select the required Registry Group and click the icon. The following confirmation dialog box is displayed.



2. Click **Yes** to delete the selected item.

Note 1: Only Registry Groups can be deleted in this interface. It is not possible to delete any Registry key under a registry group in this interface.

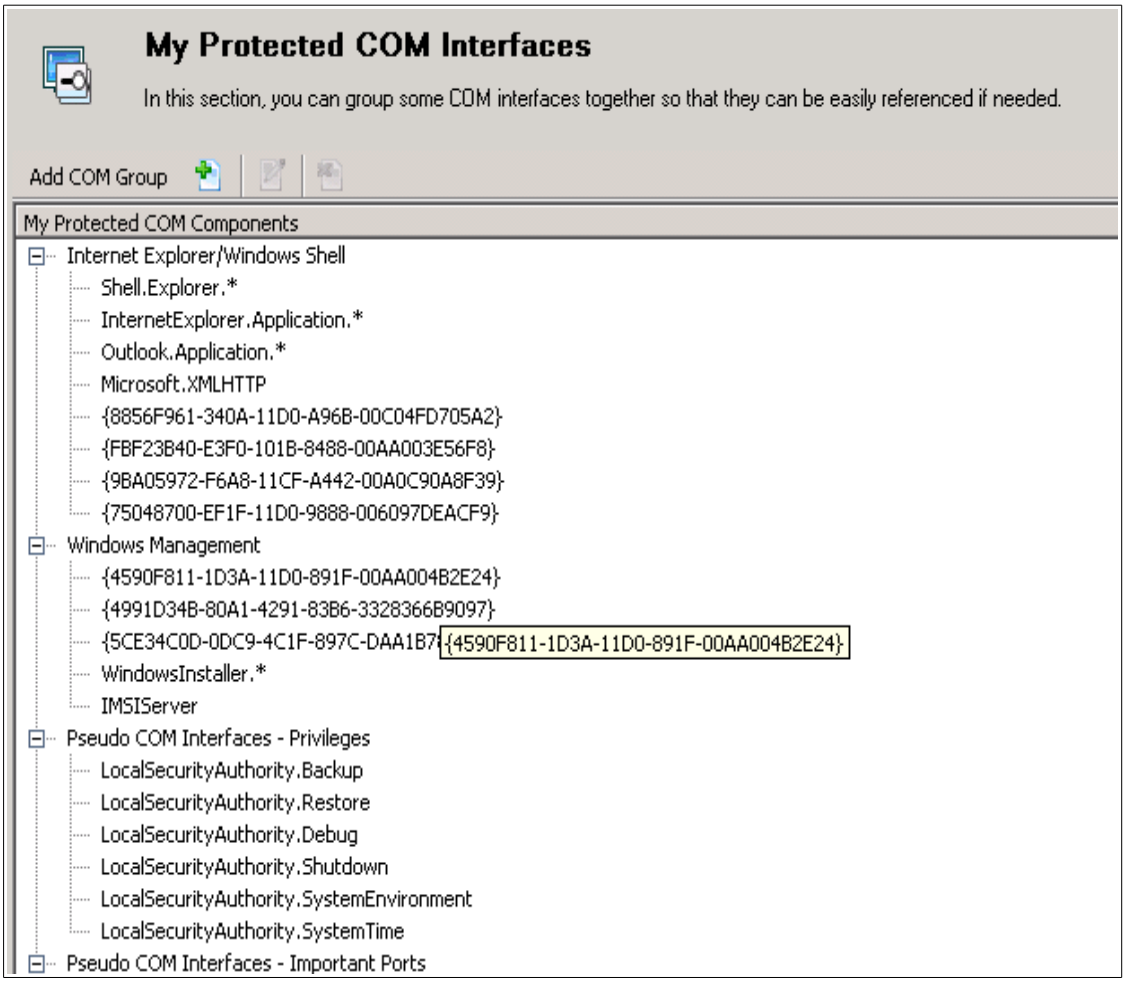
Note 2: This area is for adding existing Registry Groups only. It is not possible to to modify Registry Groups or Registry Keys from this interface.

4.2.1.4. My Protected COM Interfaces

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

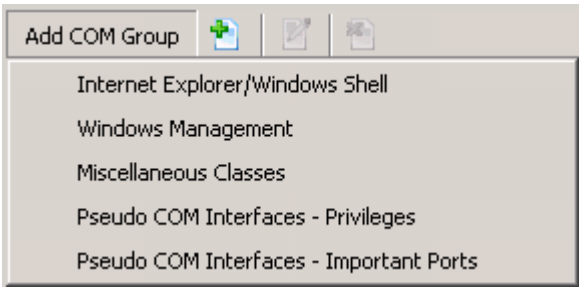
Comodo Internet Security automatically protects COM interfaces against against modification, corruption and manipulation by malicious processes.

- Click on **My Protected COM Components** in Defense+ > Common Tasks to open the 'My Protected COM Interface' interface.



To add an existing COM Group

1. Click the Add COM Group button to display the list of existing groups.

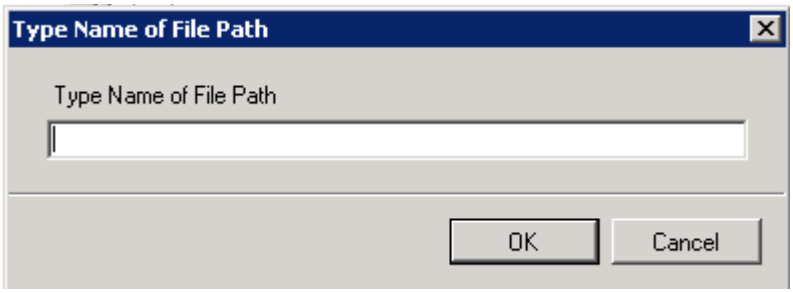


Note: The 'Add COM Group' option allows to batch select and import predefined COM interfaces.

1. Select the required COM Group from the list. The selected COM Group is displayed in the 'My Protected COM components' main list.

To add a File Path to the a COM group

1. Select the required COM group and click the icon. The 'Type Name of File Path' dialog box is displayed.

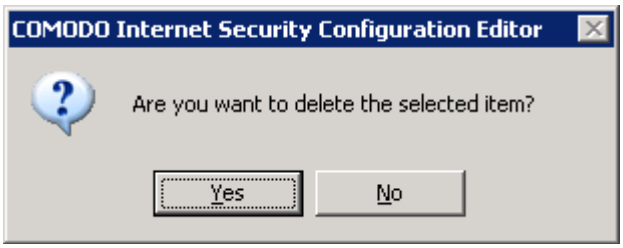


2. Type the name of the File Path.
3. Click **OK** to confirm. The name of the new file path is displayed in the main list under the selected COM group.

Note: To know how to create a new File Group and add a list of files to it, **Click here**.

To delete a COM Group

1. Select the required COM Group and click the  icon. The following confirmation dialog box is displayed.



2. Click **Yes** to delete the selected item.

Note 1: Only COM Groups can be deleted in this interface. It is not possible to delete any file path under a COM group in this interface.

Note 2: This area is for adding existing COM Groups only. It is not possible to to modify COM Groups or File Path from this interface.

4.2.1.5. My Safe Files List

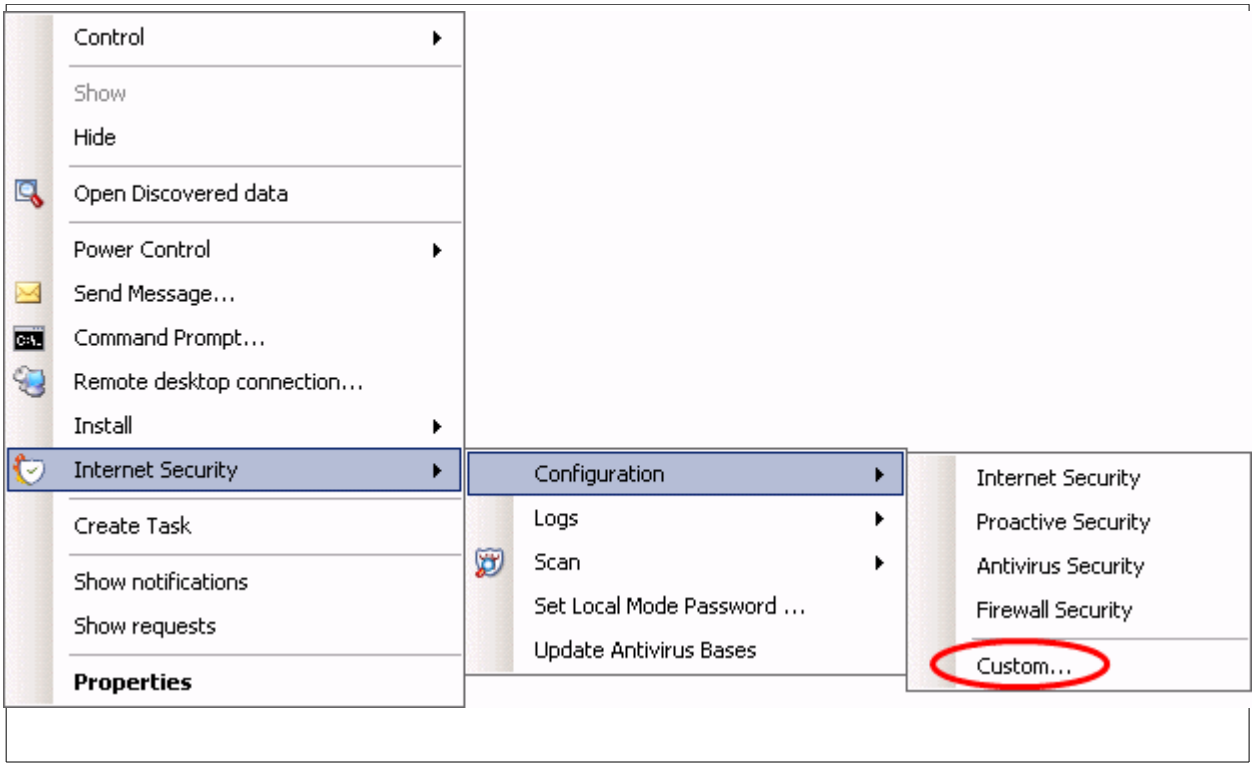
Defense+ allows the administrator to define a local safe list of files for individual CIS installations in the endpoints to complement the default Comodo safe list.

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

Important Note: The safe files list is specific for each computer and can be generated and applied for a single endpoint at a time. It cannot be created as a global safe list to apply for all or selected endpoints in a network.

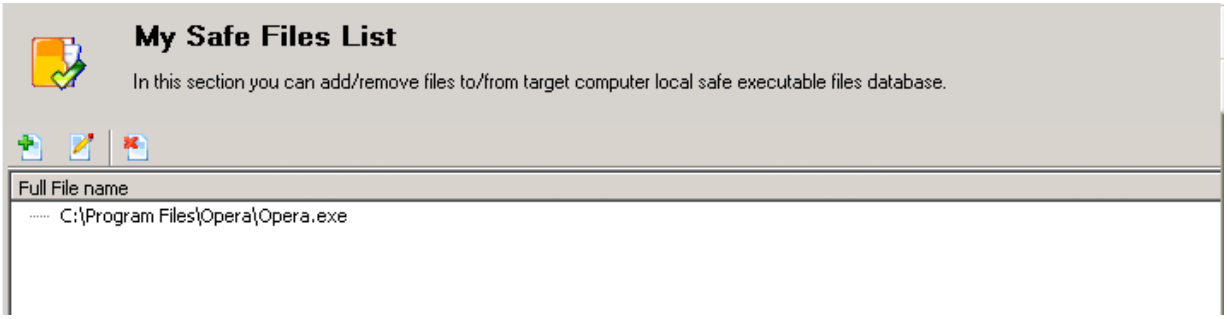
In order to set a global safe list, the administrator needs to create a Task containing a Sequence with an action CIS - Set Safe Files List and execute it on selected computers. Refer to 'The Sequence Manager Window > Table of Actions - Definitions and Usage > CIS - Set Safe Files List' section of CESM Administrators Guide for more details

The 'My Safe Files List' is available only on right clicking a computer from the Computers Window and selecting internet Security > Configuration > Custom from the context sensitive options and is not available in the configuration interface that appears when creating a sequence with the action CIS - Config.



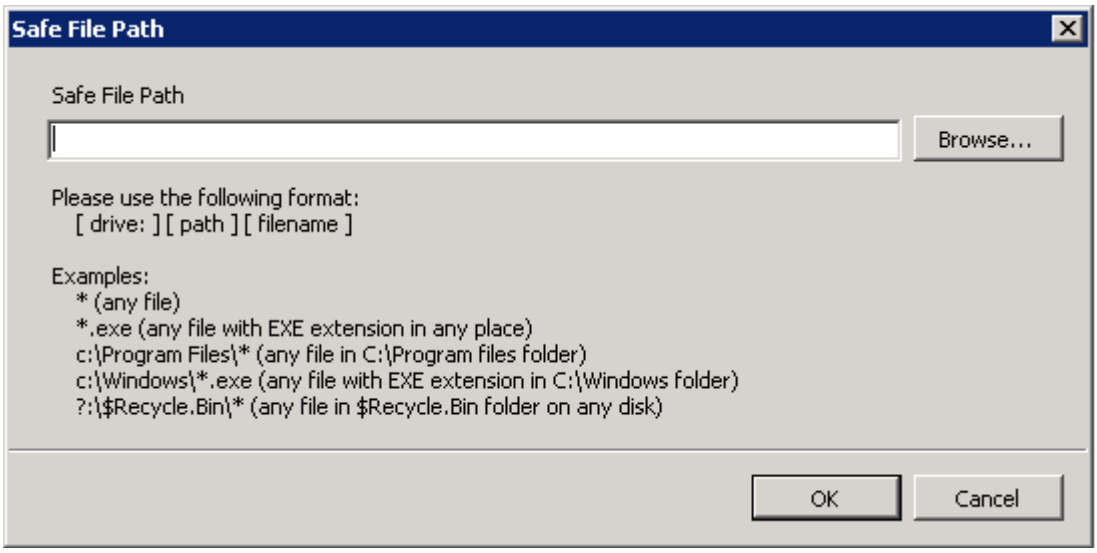
By adding executables to this list (including sub folders containing many components) the administrator can reduce the amount of requests/alerts that Defense+ generates whilst maintaining a higher level of Defense+ security. This is particularly useful for developers that are creating new applications that, by their nature, are as yet unknown to the Comodo safe list.

1. Click on **My Safe Files List** in Defense+ > Common Tasks to open the 'My Safe Files List' interface.

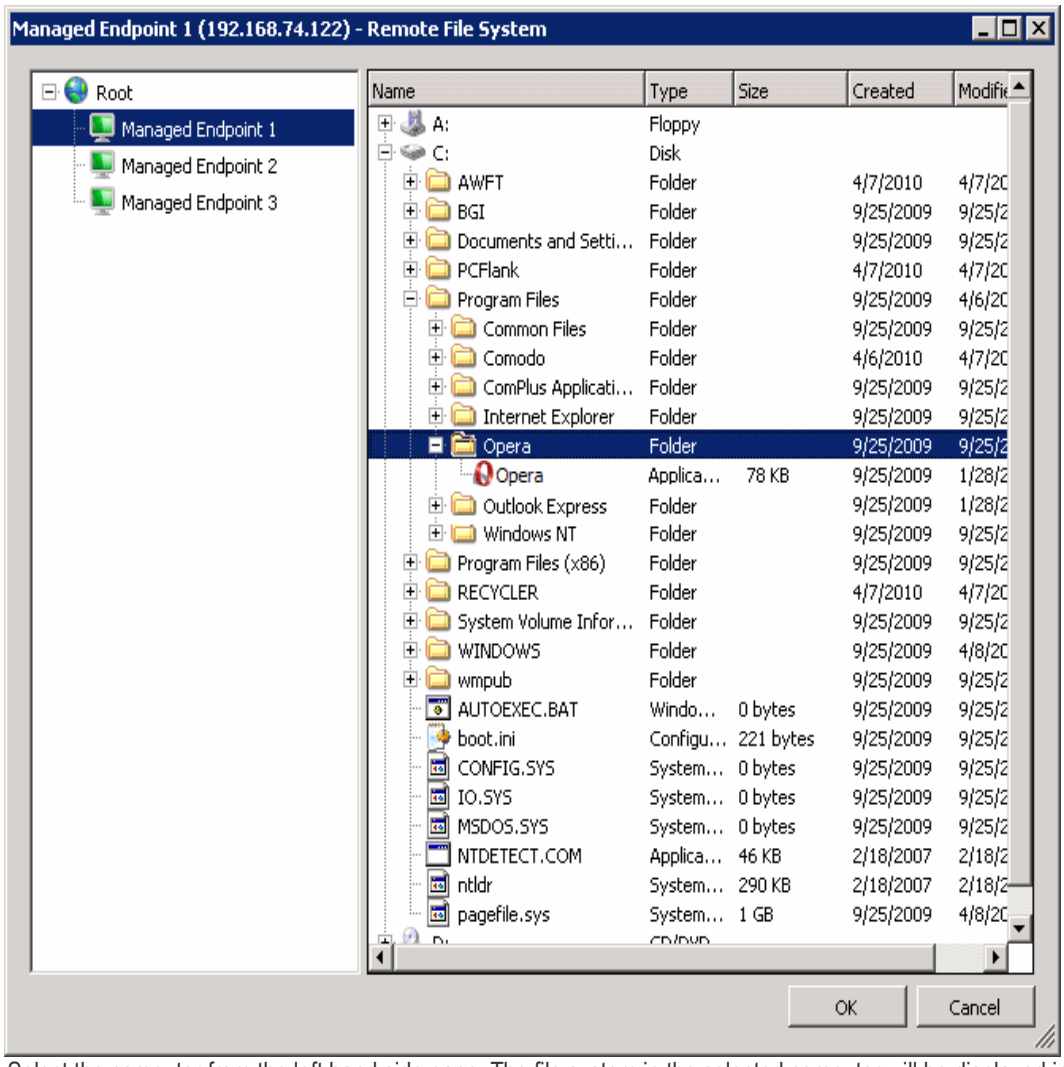


To add programs/files/executables to the My Safe Files List

1. Click the Add... icon . The Safe File Path dialog will open.



2. Type the full path of the executable in the 'Safe File Path' text box or click 'Browse'.

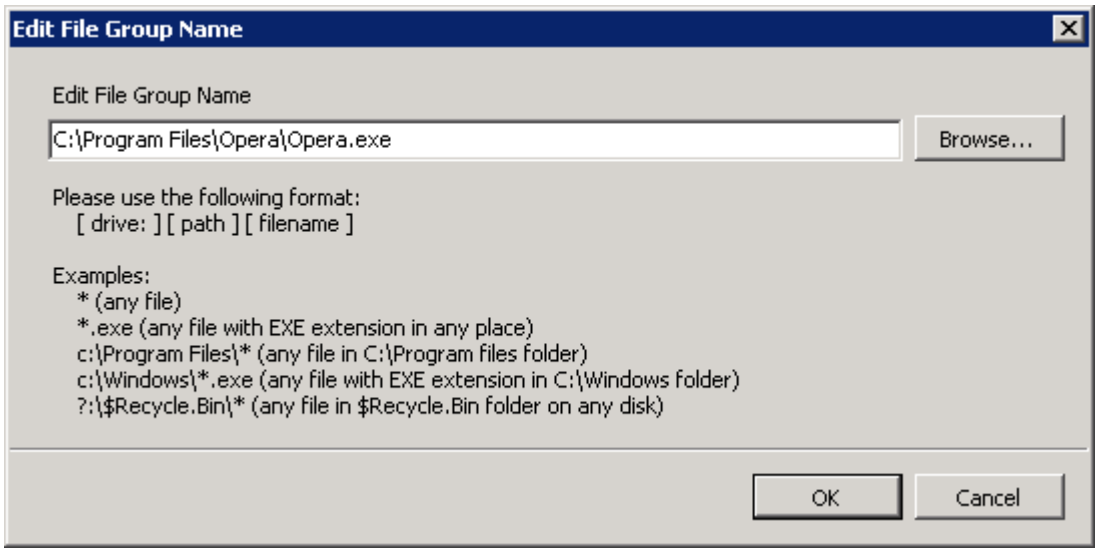


3. Select the computer from the left hand side pane. The file system in the selected computer will be displayed in the right hand side pane. Navigate to the executable and click 'OK'. The file name with the full path will now appear in the 'Safe File Path' dialog.

4. Click OK. The selected file will be added to the local safe list in the endpoint.

To edit an item in the My Safe Files List

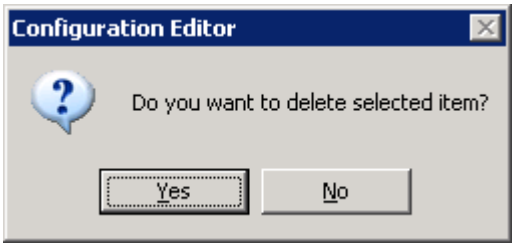
- Double click on the entry or select the entry and click the Edit icon . The Edit dialog will appear.



- Follow the process explained **above** to edit the entry.

To remove an item in the My Safe Files List

- Select the entry and click the Delete icon and click 'Yes' in the confirmation dialog.



4.2.1.6. My Trusted Software Vendors

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

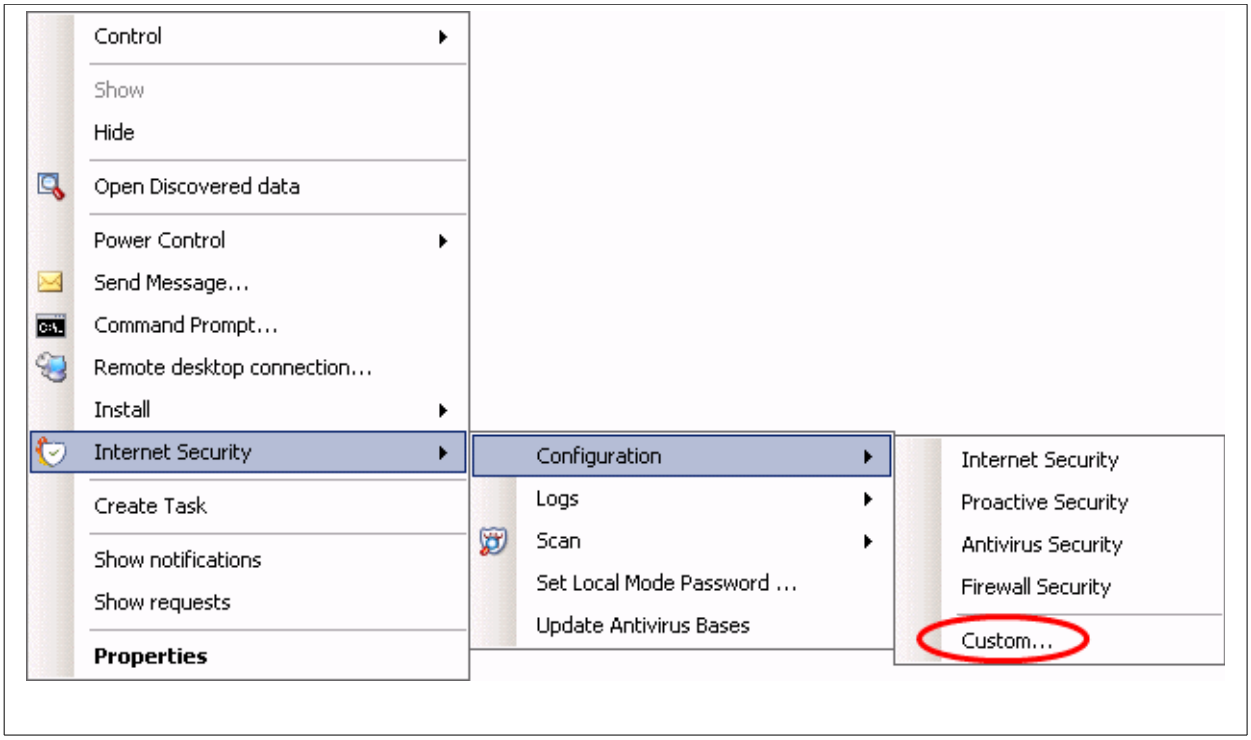
Comodo Internet Security can validate digitally signed applications from Trusted Vendors. Trusted Vendors are those companies that digitally sign 3rd party software to verify its authenticity and integrity. This signature is then countersigned by an organization called a Trusted Certificate Authority. By default, Defense+ detects software that is signed by a software vendor and counter-signed by a Trusted Certificate Authority. It then automatically adds that software to the local users' Trusted Vendor list.

Defense+ allows the administrator to define a local Trusted Vendors List for individual CIS installations in the endpoints to complement the default Trusted Vendors List.

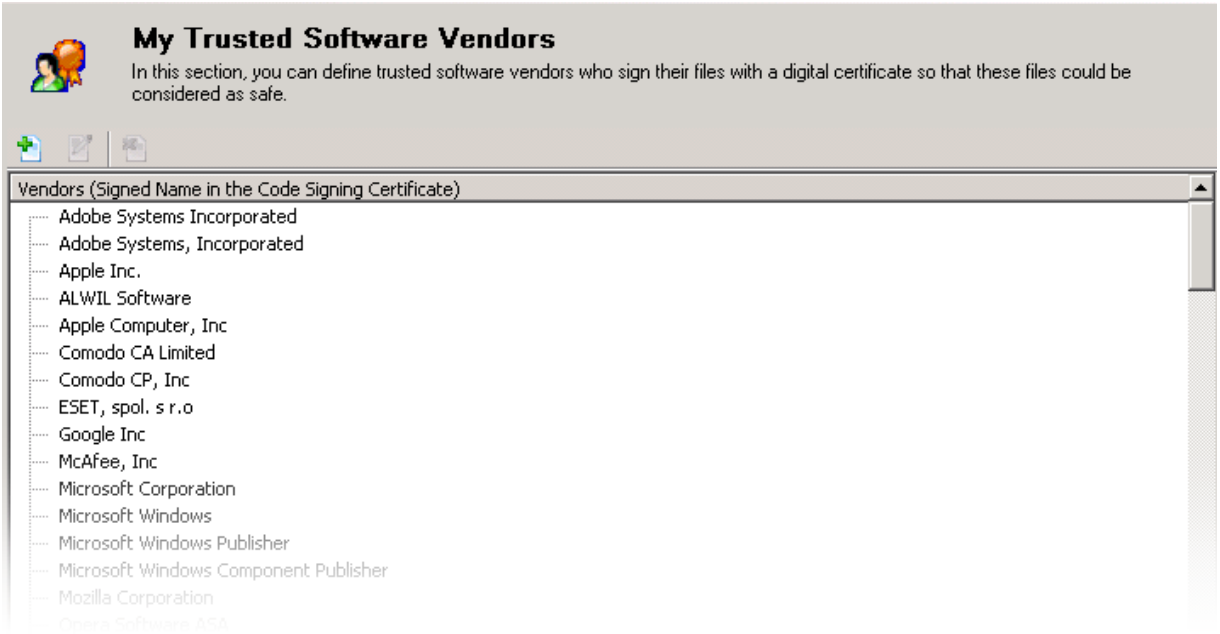
Important Note: The Trusted Vendors List generated from this option is specific for each computer and can be generated and applied for a single endpoint at a time. It cannot be created as a global Trusted Vendor List to apply for all or selected endpoints in a network.

In order to set a global Trusted Vendor List, the administrator needs to create a Task containing a Sequence with an action 'CIS - Set Trusted Vendors' and execute it on selected computers. Refer to 'The Sequence Manager Window > Table of Actions - Definitions and Usage > CIS - Set Trusted Vendors ' section of CESM Administrators Guide for more details

The 'My Trusted Software Vendors' is available only on right clicking a computer from the Computers Window and selecting internet Security > Configuration > Custom from the context sensitive options and is not available in the configuration interface that appears when creating a sequence with the action CIS - Config.



- Click on **My Trusted Vendors** in Defense+ > Common Tasks to open the 'My Trusted Software Vendors' interface.



- **Click here to read background information on digitally signing software**
- **Click here to learn how to Add / Define a user-trusted vendor**

Background

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

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

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

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

The 'Vendors' that digitally sign the software to attest to it's probity are the 3rd party software developers. These are the company names you see listed in the first column in the graphic above.

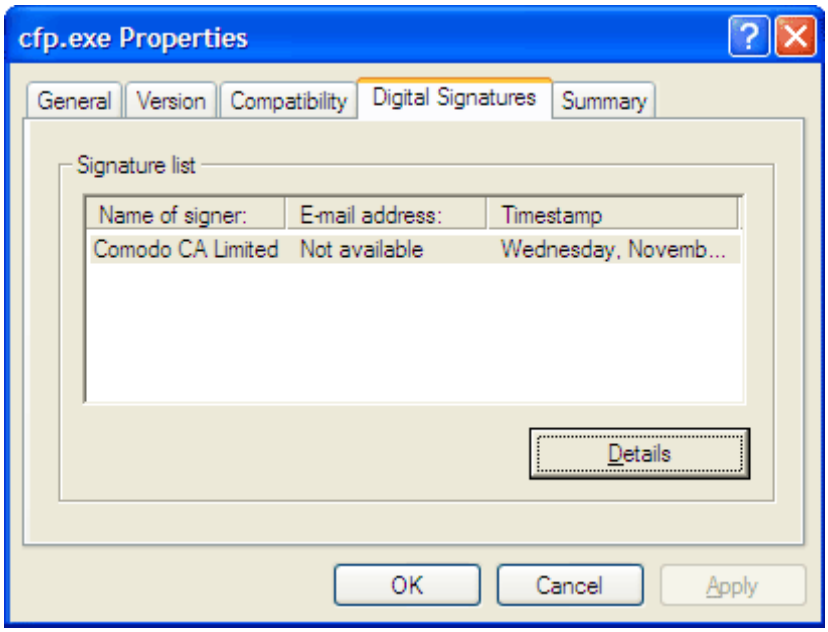
However, companies can't just 'sign' their own software and expect it to be trusted. This is why each code signing certificate is counter-signed by an organization called a 'Trusted Certificate Authority'. 'Comodo CA Limited' and 'Verisign' are two examples of a Trusted CA's and are authorized to counter-sign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

All files that are signed by the listed 'vendors' are automatically trusted by the Defense+ module of Comodo Internet Security (if you would like to read more about code signing certificates, see **http://www.instantssl.com/code-signing/**).

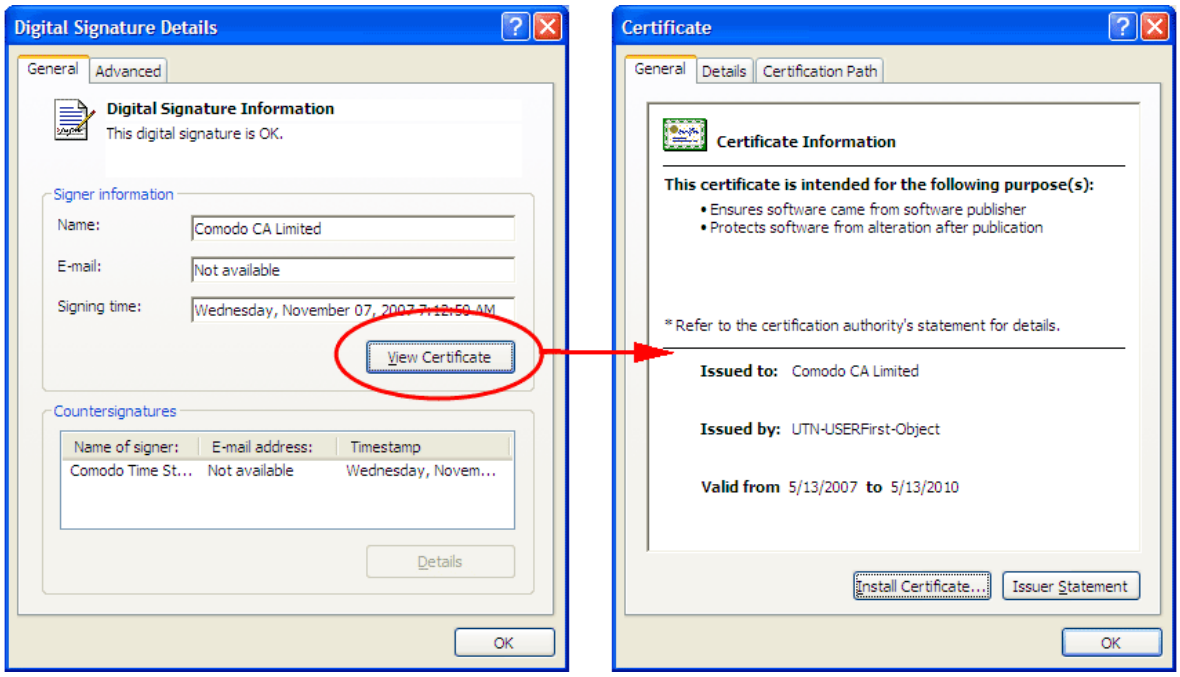
One way of telling whether an executable file has been digitally signed is checking the properties of the .exe file in question. For example, the main program executable for Comodo Internet Security is called 'cfp.exe' and has been digitally signed.

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

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



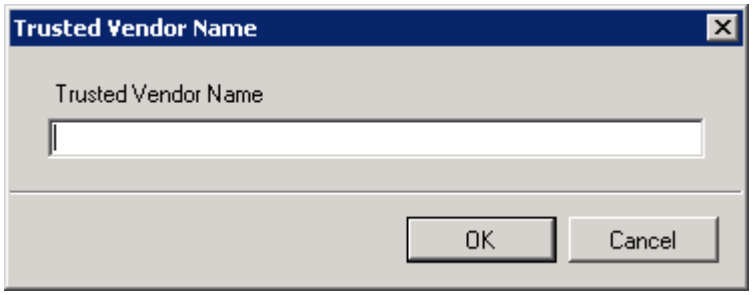
Click the 'Details' button to view digital signature information. Click 'View Certificate' to inspect the actual code signing certificate. (see below)



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

To add a Trusted Vendor to the list

1. Click the Add... icon . The 'Trusted Vendor Name' dialog will open.



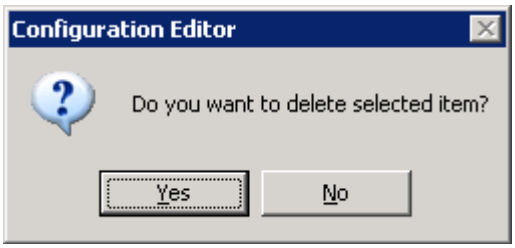
2. Type the name of the vendor in the Trusted Vendor Name text box and click OK. The Trusted Vendor will be added to the list.

To edit a Trusted Vendor Name

- Double click on the name or select the name and click the Edit icon . he 'Trusted Vendor Name' dialog will appear. Edit the name in the 'Trusted Vendor Name' text box.

To remove edit a Vendor Name from the list

- Select the vendor name and click the Delete icon and click 'Yes' in the confirmation dialog.



4.2.2. The Sandbox

Comodo Internet Security's new sandbox is an isolated operating environment for unknown and untrusted applications. Running an application in the sandbox means that it cannot make permanent changes to other processes, programs or data on the 'real' system. Comodo have integrated sandboxing technology directly into the security architecture of CIS to complement and strengthen the Firewall, Defense+ and Antivirus modules. Applications in the sandbox are executed under a carefully selected set of privileges and writes to a virtual file system and registry instead of the real system. This delivers the smoothest user experience possible by allowing unknown applications to run and operate as they normally would while denying them the potential to cause lasting damage.

After an unknown application has been placed in the sandbox, CIS also automatically queues it for submission to Comodo labs where it is analyzed by our technicians. If it is found to be harmless then it is added to the global safe list that is downloaded by all CIS users in the next round of updates. Once it is added to the safe list, the application is no longer run in the sandbox by CIS (unless the user explicitly places it there). Conversely, if the application is found to be malicious then it is added to Comodo's list of malware signatures and is deleted after the next round of updates. The obvious benefit here is that the malware was not able to wreak any damage in the meantime.

By uniquely deploying 'sandboxing as security', CIS offers improved security, fewer requests/alerts and greater ease of use than ever before.

4.2.2.1. The Sandboxing Process

- When an executable is first run it passes through the following CIS security inspections:
  - Antivirus scan
  - Defense+ Heuristic check
  - Buffer Overflow check
- If the processes above determine that the process is malware then the administrator/user is alerted
- An application can become recognized as 'safe' by CIS (and therefore not sandboxed) in the following ways:
  - Being on the global Comodo Safe List
  - By the user adding the application to the local '**My Safe Files List**'
  - By the user granting the installer elevated privileges (CIS detects if an executable requires administrative privileges. If it does, it raises a request/alert. If the administrator/user choose to trust, CIS regards the installer and all files generated by the installer as safe)
- Additionally, a file is not sandboxed if it is defined as an Installer or Updater in HIPS policy (See **Computer Security Policy** for more details)
- Applications that pass the security inspections but are not yet recognized as 'safe' will be sandboxed. CIS will alert the administrator/user that it is going to run the application in the sandbox.
- The decision making process outlined above is taken each time the application is run.
- Automatically sandboxed applications are run with 'Limited' restrictions.

More Info: Sandboxed applications are allowed to run under a specific set of conditions or privileges. In CIS, these are known as 'Restriction Levels'. There are four levels - Unrestricted, Limited, Restricted and Untrusted ('Limited' is the default level for applications that are automatically placed in the sandbox). In part, sandbox restriction levels are implemented by enforcing or relaxing the native access rights that Windows can grant to an application. For example, the 'Limited' setting applies some of the supported operating system restrictions and grants it access rights similar to if the application was run under a non-admin user account. These restriction levels are fortified with certain Defense + restrictions that apply to all sandboxed applications (for example, they cannot key log or screen grab, set windows hooks, access protected COM interfaces or access

non-sandboxed applications in memory. If the user disables virtualization, then sandboxed apps. can't modify registry keys or modify existing protected files either.)

- Applications can be placed in the sandbox automatically by CIS or by the **Programs in the Sandbox**.
- Automatically sandboxed applications cannot be viewed or modified in the interface. Applications that were automatically sandboxed can only be removed if they become recognized as 'safe' by CIS (see conditions above).
- A sandboxed application will also be submitted to Comodo. If found to be safe, it will be auto-removed from the sandbox and allowed to access the 'real' environment.
- Sandboxed applications do not produce any Antivirus, Firewall or Defense+ Alerts.

Other notes

- If a safe or installer application is executed by an application running inside the sandbox, the installer also runs in the sandbox no matter what.
- If a user defines an application for sandboxing, this causes any applications (safe or installer) to also be executed inside the sandbox.
- In addition to the Sandbox restriction level set for an application, Defense + also implements the following restrictions. A sandboxed application cannot:
  - Access non-sandboxed applications in memory
  - Access protected COM interfaces
  - Key log or screen capture
  - Set windows hooks
  - Modify protected registry keys (if virtualization is disabled)
  - Modify EXISTING protected file (if virtualization is disabled).

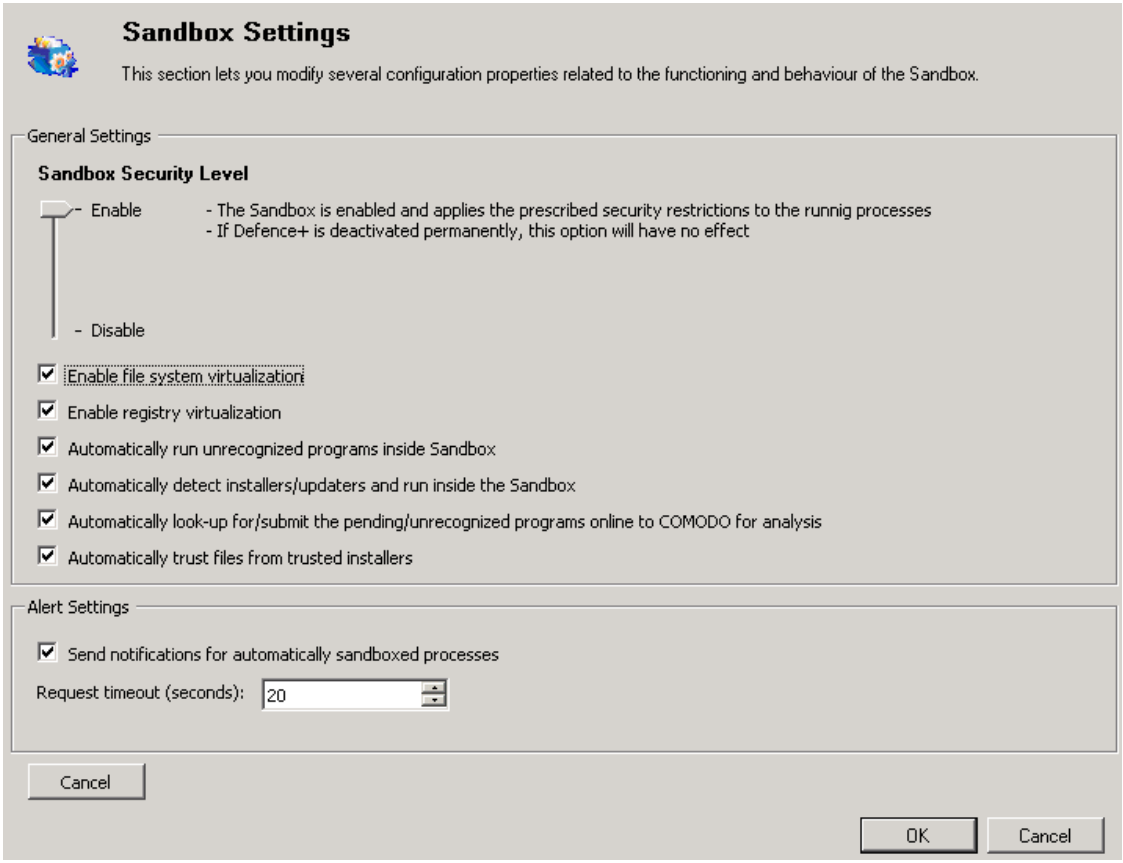
The 'Sandbox' area can be accessed by clicking the 'Sandbox' link under Defense +. Click the links below for detailed explanations of the options in this section.

- **Sandbox Settings**
- **Files**

4.2.2.2. Sandbox Settings

The Sandbox Settings area allows the administrator to configure the security level and the overall behavior of the sandbox. To access the Sandbox Settings interface, click the Sandbox Settings link under Sandbox in Defense+ area. Sandbox settings are split into two areas. Click on either of the links to jump straight to that sections.

- **General Settings** - Allows you to enable or disable the sandboxing feature and configure various sandbox related settings.
- **Alert Settings** - Allows you to configure requests/alerts from the sandbox feature.



General Settings

Security Level Slider

The Security Level slider in the Settings interface allows you to switch the Sandbox between **Enabled** and **Disabled** states. The programs included in the Sandbox is executed with the set restrictions only if the Sandbox is in Enabled state. If disabled, the programs is run normally without any restrictions. The Sandbox is disabled irrespective of the settings in this slider, if Defense+ is **permanently deactivated** from the **Defense+ Settings** interface.

Check Boxes

Enable file system virtualization - The sandboxed applications are not permitted to modify the files in your 'real' file system. Enabling file system virtualization instructs the Sandbox to create a virtual file system in the endpoint system. The sandboxed applications will write any data only into the created virtual file system, instead of affecting and potentially causing damage to the real file system. If this option is disabled, the sandboxed applications may not function correctly because they will not be able to create the entries that they need too.

Note for advanced users: The virtual file system is created inside the Sandbox working folder (e.g. c:\sandbox\) to execute the applications within this file system.

If you disable this option here, the virtual file system is not created even if you have **enabled file system virtualization** for individual applications within the Sandbox.

Enable registry virtualization -The sandboxed applications are not permitted to access and modify the entries in the 'real' Window's Registry hives. Enabling registry virtualization instructs the Sandbox to create a virtual registry hive in the system. The sandboxed applications write any entries pertaining to them only into the created registry hive, instead of affecting and potentially causing damage to the real registry hives. If this option is disabled, the sandboxed applications may not function correctly because they are not able to create the entries that they need too.

Note for advanced users: The virtual registry hive is created as HKEY_LOCAL_MACHINE\SYSTEM\Sandbox\ ... for the sandboxed applications to write their registry values. If you disable this option here, the virtual registry hive is not created even if you have **enabled file system virtualization** for individual applications within the Sandbox.

The table below explains the precedence of the file system virtualization and registry virtualization settings made through this interface and those through **Adding programs to run inside the Sandbox > Advanced Settings.**

Sandbox Settings	Add programs to run inside the Sandbox > Advanced Settings	Is the setting enabled for the specific application?
Yes	Yes	Yes
Yes	No	No
No	Yes	No
No	No	No

Automatically run unrecognized programs inside the Sandbox - If any executable which is not recognized by COMODO is attempted to run, the application is automatically executed within the Sandbox to safeguard the other files/applications in the system. For the applications run within the Sandbox automatically:

- Maximum of only one third of the system memory can be allocated;
- The Restriction level is set to 'Limited'. (**Click here** for more details on 'Limited' restriction level).

Exceptions -

An application is not sandboxed automatically if it is defined as an Installer or Updater in **Computer Security Poilcy** under Defense+ Tasks > Advanced Tasks.

An application is not sandboxed automatically if it is an installer or an application that requires administrative privileges. On execution of such applications, a 'Run with elevated privileges' request/alert is raised. The administrator can allow or block it depending on the trustworthiness of the publisher / vendor from the alert dialog. Depending on the response, CIS trusts that publisher / vendor and allow all the files from the same publisher / vendor in future.

Automatically detect the installers/updaters and run them outside the Sandbox - On execution of an Installer or an Updater, the application is run outside the Sandbox. Select this option only if you are going to run installers/ updaters from trusted vendors.

Automatically look-up /submit the pending/unrecognized programs online to COMODO for analysis - Instructs the Sandbox to monitor all the unrecognized files in the system and to initiate the file submission process automatically. The files are analyzed by Comodo technicians and added to the safe list or black list accordingly.

Automatically trust the files from the trusted installers - Files that are generated by trusted installers are also trusted. This means that they will not be sandboxed.

Alert Settings

Send Notifications for automatically sandboxed processes - By default, CIS will send a notification to the Administration Console whenever it runs an unknown application in the sandbox. Use this control to enable or disable these notifications.

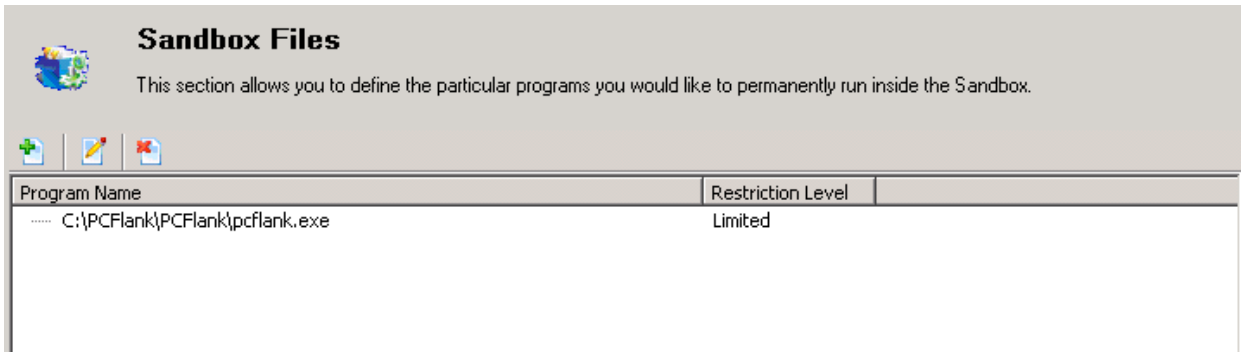
Request timeout (seconds) - Enables the Administrator to specify the length of time (in seconds) for a request/alert generated by sandbox to expire.

4.2.2.3. Applications Running inside Sandbox

The 'Files' area lists those applications which the administrator has decided to be executed in the sandbox on a permanent or long term basis. This may include applications that the user suspects are not safe or has other concerns about (for example, the end user may wish to test beta software by running it in the sandbox). These applications will appear as normal programs in the

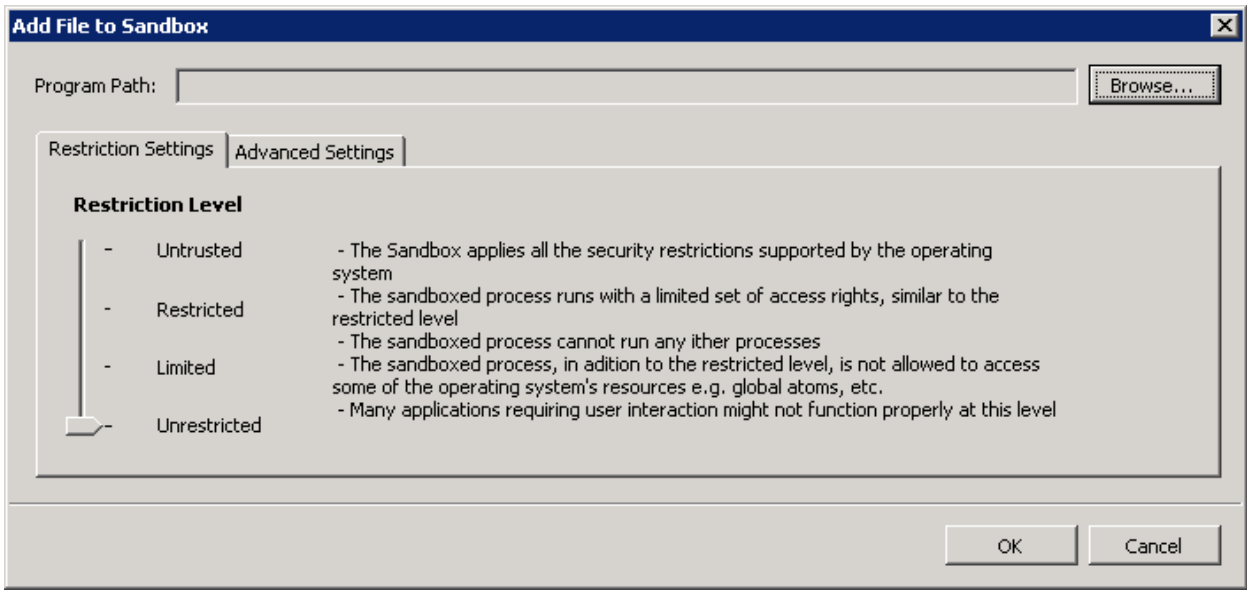
system but will be run in the sandbox under a restricted set of privileges. They will not be allowed to access files on the real system, alter operating system settings or alter the registry entries corresponding to other applications.

The Files area can be accessed by clicking the 'Files' link under Sandbox in the Defense+ area.

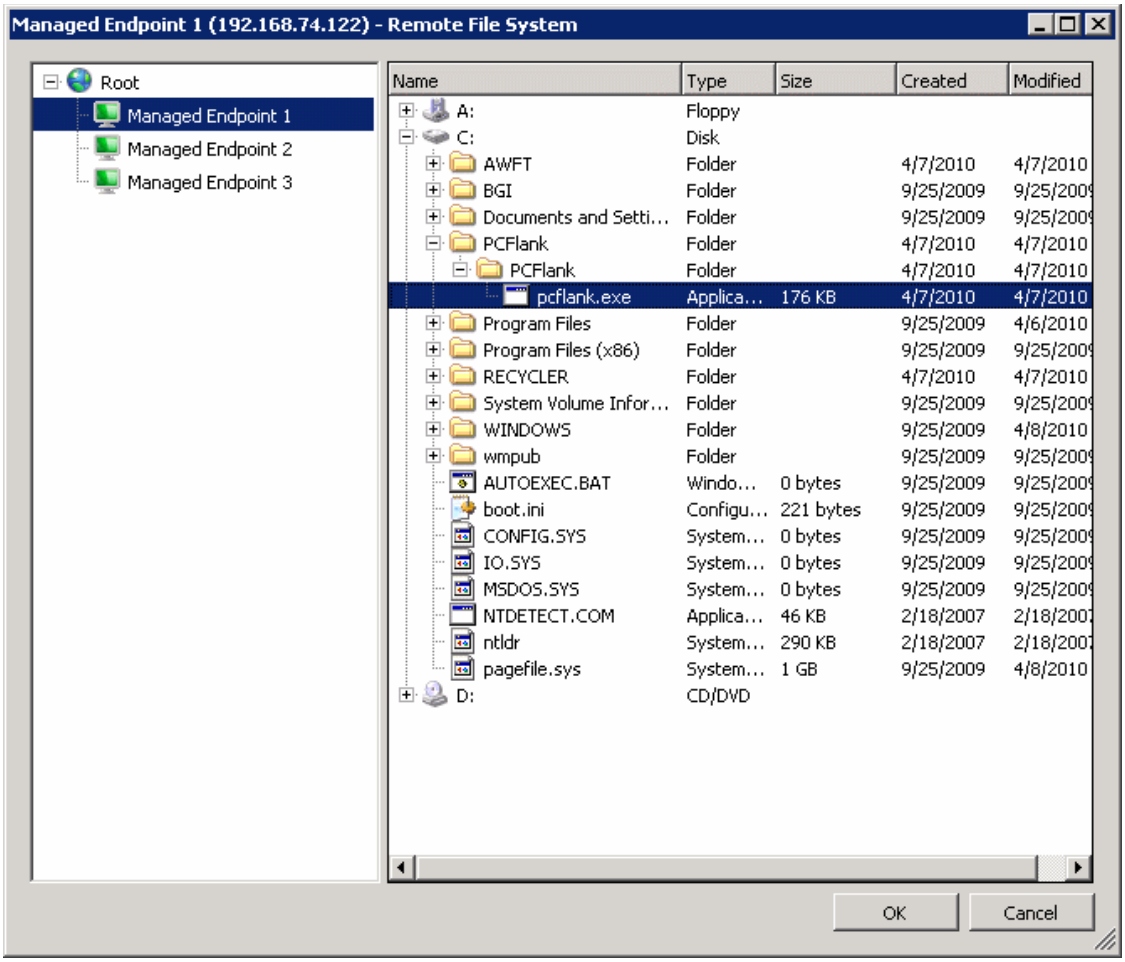


Adding programs to run inside the Sandbox

1. Click the Add... icon . The 'Add File to Sandbox' dialog appears.



2. Click 'Browse'.



3. Select the computer from the left hand side pane. The file system in the selected computer will be displayed in the right hand side pane. Navigate to the executable and click 'OK'. The file name with the full path will now appear in the 'Add File to Sandbox' dialog.
4. Choose 'Restriction Settings'

i. **Untrusted** - The application is not allowed to access any of the Operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. The restrictions on usage of system memory, operation with virtual file system and registry and execution time defined in **Advanced Settings** is imposed.

Note: Some of the applications that require user interaction may not work properly under this setting.

ii. **Restricted** - The application is allowed to access very few Operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. The restrictions on usage of system memory, operation with virtual file system and registry and execution time defined in **Advanced Settings** is imposed.

Note: Some of the applications like computer games may not work properly under this setting.

iii. **Limited** - Only selected Operating System resources can be accessed by the application. The application is not allowed to execute more than 10 processes at a time and is run with out Administrator account privileges. The restrictions on usage of system memory, operation with virtual file system and registry and execution time defined in **Advanced Settings** is imposed.

iv. **Unrestricted** - No Operating System restrictions is applied - meaning the application is allowed to access all the Operating system files and resources like clipboard. Still the restrictions on usage of system memory, operation with virtual file system and registry and execution time defined in **Advanced Settings** is imposed.

5. Choose 'Advanced Settings'

The Advanced Settings tab to configure the restrictions on system resource usage and access to other files. Available options are:

i. Limit maximum memory consumption - You can define how much of the system memory can be allocated for the application on execution by selecting this checkbox and entering the memory (in MB) in the combo box beside it.

ii. Limit the program execution time - You can define how long the program can be allowed to run by selecting this checkbox and entering the time (in seconds) in the combo box beside it.

iii. Enable file system virtualization -The sandboxed applications are not permitted to modify the files in your 'real' file system. Enabling file system virtualization instructs the Sandbox to create a virtual file system in your system. The application added to the sandbox writes any data only into the created virtual file system, instead of affecting and potentially causing damage to your real file system. If you disable this option, the application may not function correctly because it is not be to create the entries that it needs too.

Note for advanced users: The virtual file system is created inside the Sandbox working folder (e.g. c:\sandbox\<application name>) to execute the application within this file system.

The virtual file system is not created even on enabling this setting here, if file system virtualization is disabled in **Sandbox Settings**.

iv. Enable registry virtualization - The sandboxed applications are not permitted to access and modify the entries in your 'real' Window's Registry hives. Enabling registry virtualization instructs the Sandbox to create a virtual registry hive in your system. The application added to the Sandbox writes any entries pertaining to it only into the created registry hive, instead of affecting and potentially causing damage to your real registry hives. If you disable this option, the application may not function correctly because it is not able to create the entries that it needs too.

Note for advanced users: The virtual registry hive is created as HKEY_LOCAL_MACHINE\SYSTEM\Sandbox\ ... for the sandboxed applications to write their registry values.

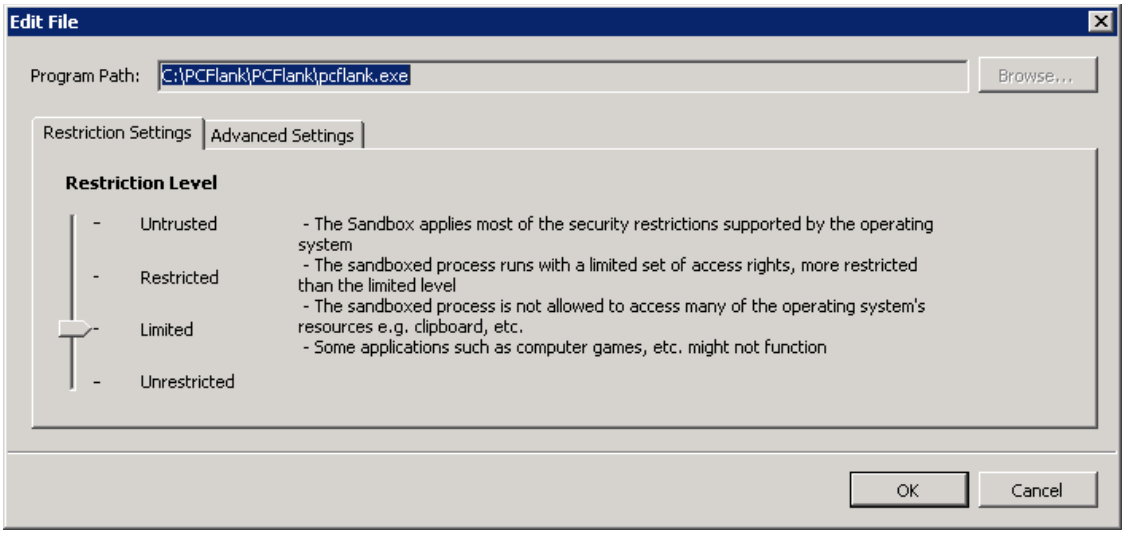
The virtual registry hive is not created even on enabling this setting here, if registry virtualization is disabled in **Sandbox Settings**.

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

From this point onwards the application will be run in the sandbox.

To edit the Restriction Settings/Advanced Settings for an application in the sandbox

Double click on the application or click the edit icon  . The edit File dialog will appear.



Edit the settings as explained **above**.

To remove an application from the sandbox

- Select the application and click the Delete icon  . Click Yes in the confirmation dialog'
- Next time you execute this application it will run outside of the sandbox (presuming it is not then detected as malicious or automatically sandboxed as **per the sandboxing process**)
- Advanced Tasks

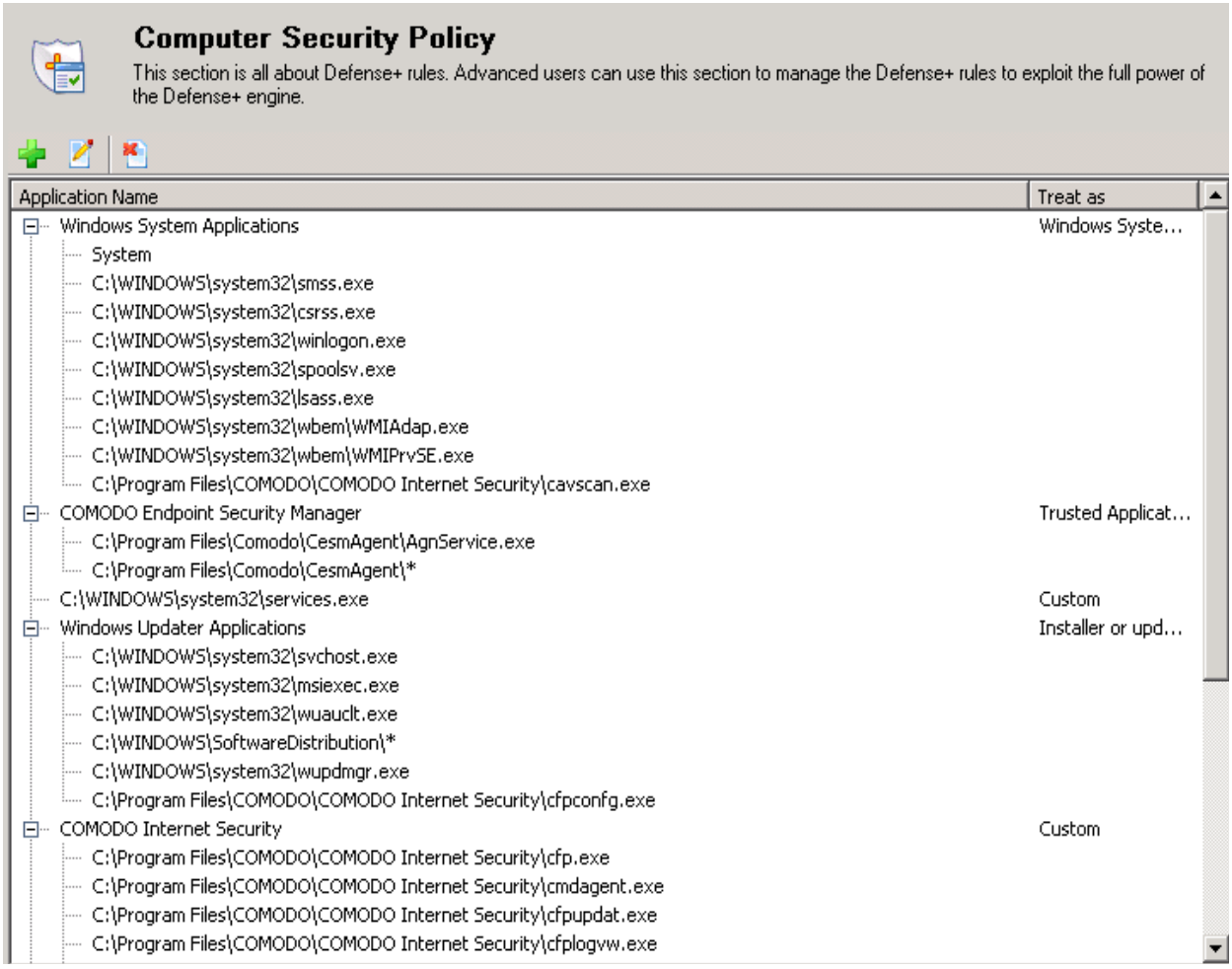
'Advanced Tasks' enables more experienced administrators to define Defense+ security policy and settings at an in-depth, granular level. Click on the links below to see detailed explanations of each area in this section.

- **Computer Security Policies**
- **Predefined Security Policies**
- **Image Execution Control Settings**
- **Defense+ Settings**

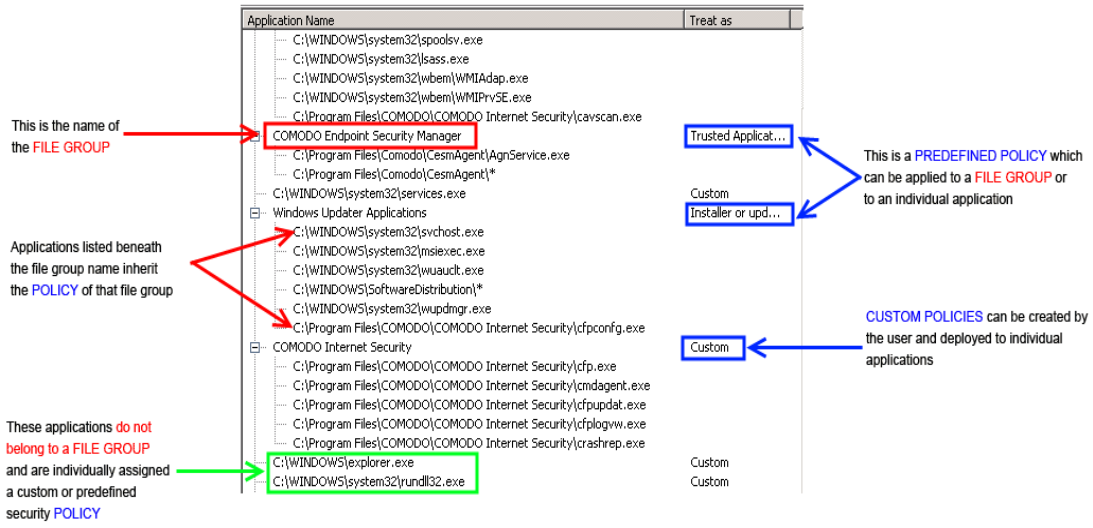
4.2.2.4. Computer Security Policy

The Computer Security Policy area allows the administrator to view manage and edit the Defense+ security policies that apply to applications.

- Click on **Computer Security Policy** in Defense+ > Advanced Task to open the 'Computer Security Policy' interface.



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



General Navigation controls for Computer Security Policy interface:

Window Specific Navigation Controls - Computer Security Policy		
Menu Element	**Element Icon**	**Description**
Add New Group		Allows the administrator to Add a new Application to the list then create it's policy. See the section '**Creating or Modifying a Defense+ Security Policy**'.
Edit		Allows the administrator to modify the Defense+ security policy of the selected application. See the section '**Creating or Modifying a Defense+ Security Policy**'.
Remove		Deletes the current policy. **Note**: Individual applications cannot be removed from a file group using this interface - use the '**My File Groups**' interface to do this.

Administrators can re-order the priority of policies by simply dragging and dropping the application name or file group name in question. To alter the priority of applications that belong to a file group, use the **'My File Groups'** interface.

Creating or Modifying a Defense+ Security Policy

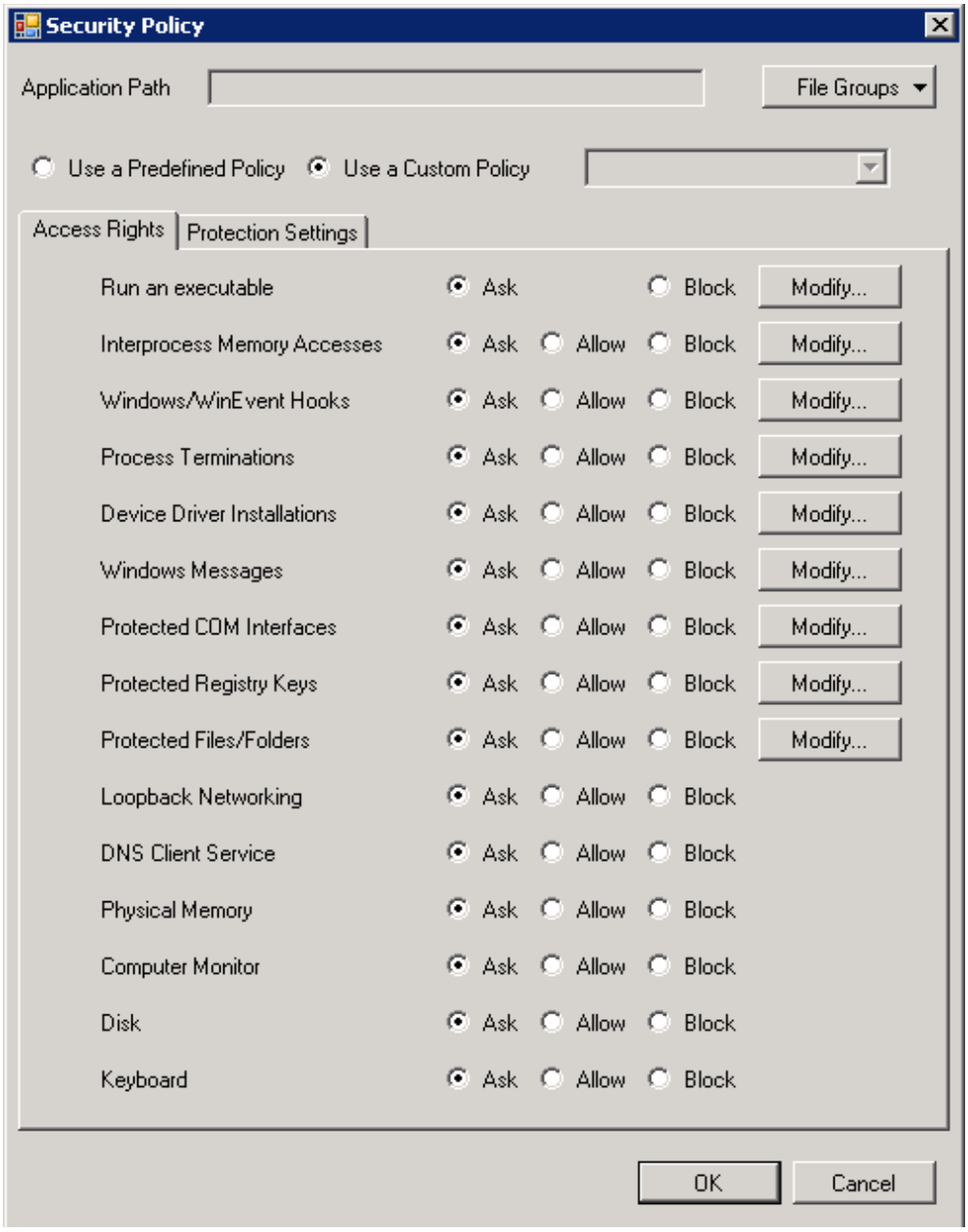
To begin defining a application's Defense+ policy,

(1) Select the application or file group that needs to be applied to the policy.

(2)Configure the security policy for this application.

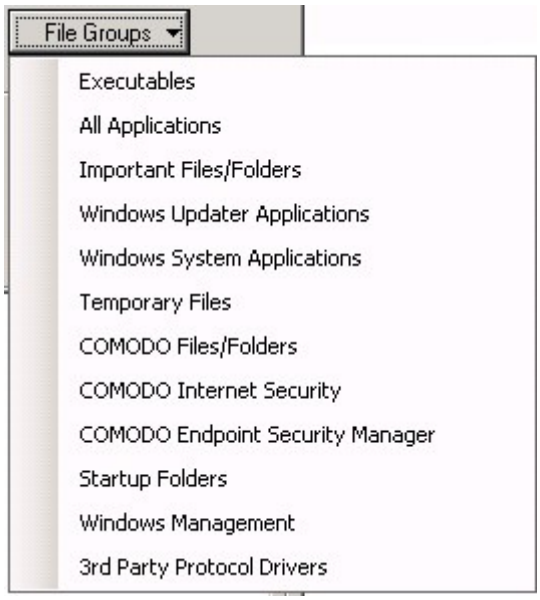
(1) Select the application or file group that needs to be applied to the policy

- Click the  icon in the main **Computer Security Policy interface**. This opens the **Security Policy** dialog box shown below:



Note: As this is a new application, the 'Application Path' field is blank. While modifying an existing policy, this interface shows the individual rules for that application's policy.

- Click **File Groups** button.



- Select the required Application Path from the drop down.

The **File Groups** option allows to create a Defense+ security policy for a category of preset files or folders. For example, selecting 'Executables' would enable the administrator to create a Defense+ policy for all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl . Other such categories available include 'Windows System Applications' , 'Windows Updater Applications' , 'Start Up Folders' etc - each of which provide a fast and convenient way to apply a generic policy to important files and folders.

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

The 'My File Groups interface can be accessed either of the following methods:

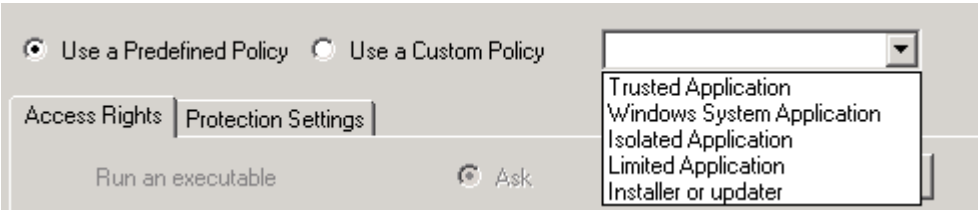
Navigate to Defense+ > Common Tasks > My Protected Files then click the 'My Groups' button.

(2)Configure the Security Policy for this application

There are two broad options available for selecting a policy that apply to an application - **Use a Pre-defined Policy** or **Use a Custom Policy**

(i) Use a Predefined Policy -

- Select this option to quickly deploy an existing policy on to the target application.
- Choose the policy from the drop-down menu. The name of the predefined policy is displayed in the **Treat As** column for the selected application in the **Computer Security Policy** interface.



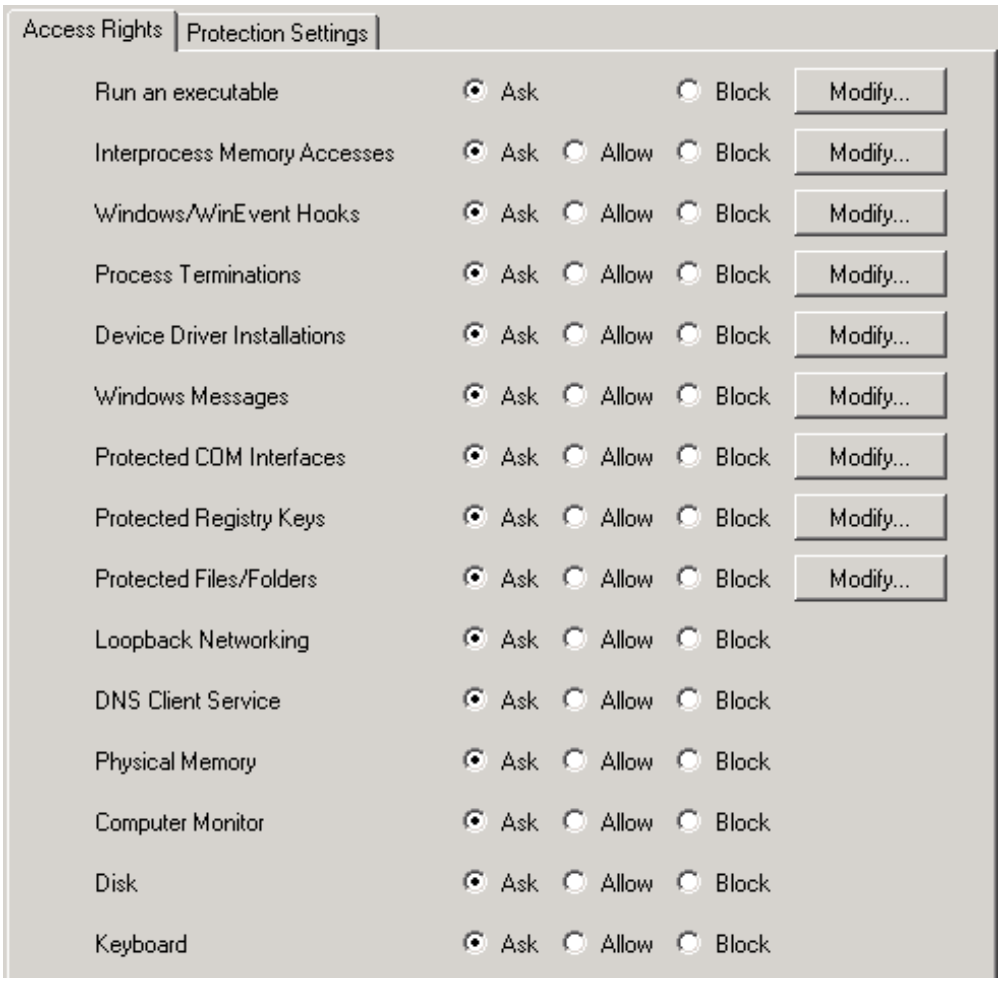
Note: It is not possible to modify Predefined Policies ***directly*** from this interface - they can only be modified and defined using the **Predefined Security Policies** interface. To add or modify rules for an application means creating a new custom policy and should be done using the more flexible **Use Custom Policy** option.

(ii) Use a Custom Policy: Designed for more experienced administrators. The Custom Policy option has two main configuration areas - **Access Rights** and **Protection Settings**. In simplistic terms 'Access Rights' determine what the application *can do* to other processes and objects whereas 'Protection Settings' determine what the application *can have done to it* by other processes.

- Select this option to enable full control over the configuration of specific security policy and the parameters of each rule within that policy.

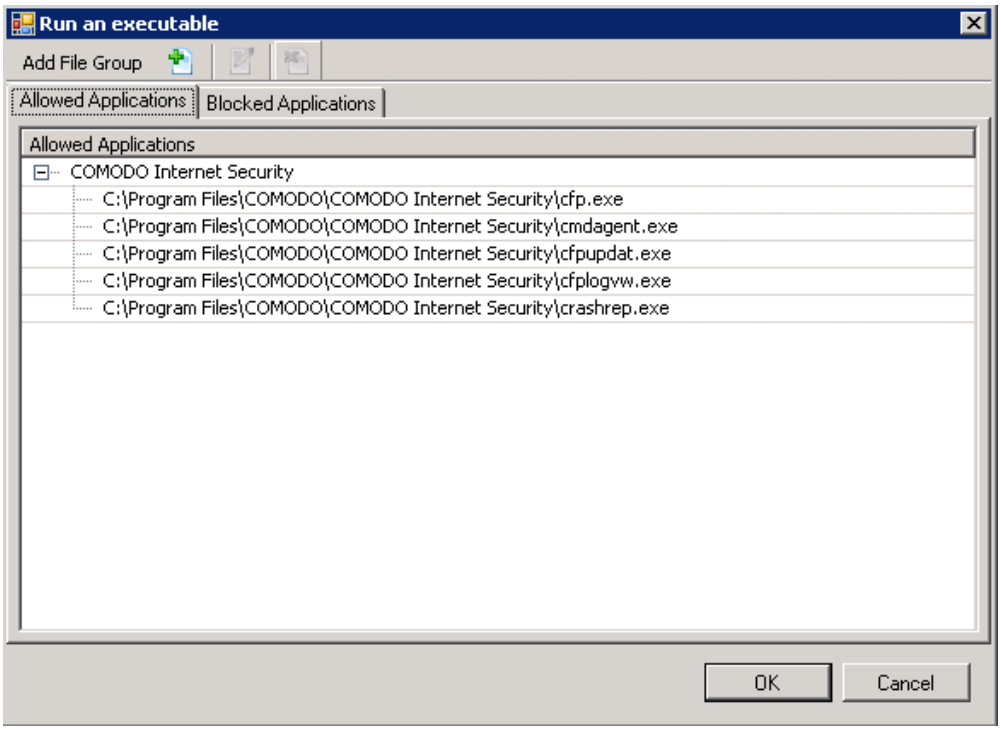
Note: Selecting the Use a Custom Policy option enables the **Access Rights** tab and **Protection Settings** tab.

Access Rights - The Process Access Rights interface allows to determine what activities the applications in the custom policy are allowed to execute. These activities are called 'Access Names'.



Tip: **Click here** to view a list of definitions of the **Action Names** listed above and the implications of choosing to Ask, Allow or Block for each setting.

- Select 'Ask', 'Allow' or 'Block' option for the respective Action name.
- Click the **Modify** button to specify the policy exceptions for 'Ask', 'Allow' or 'Block' option. This opens the **Run an executable** dialog box.



- Select the **Allowed Applications** or **Blocked Applications** tab depending on the type of exception that needs to be created.
- Click Add File Group to choose and apply this exception to the selected applications or file groups.

Tip: **Click here** for an explanation of available options.

- Select the required File Group from the list. The selected File Group is displayed in the 'My Protected Files' main list.

To add a File to a file group

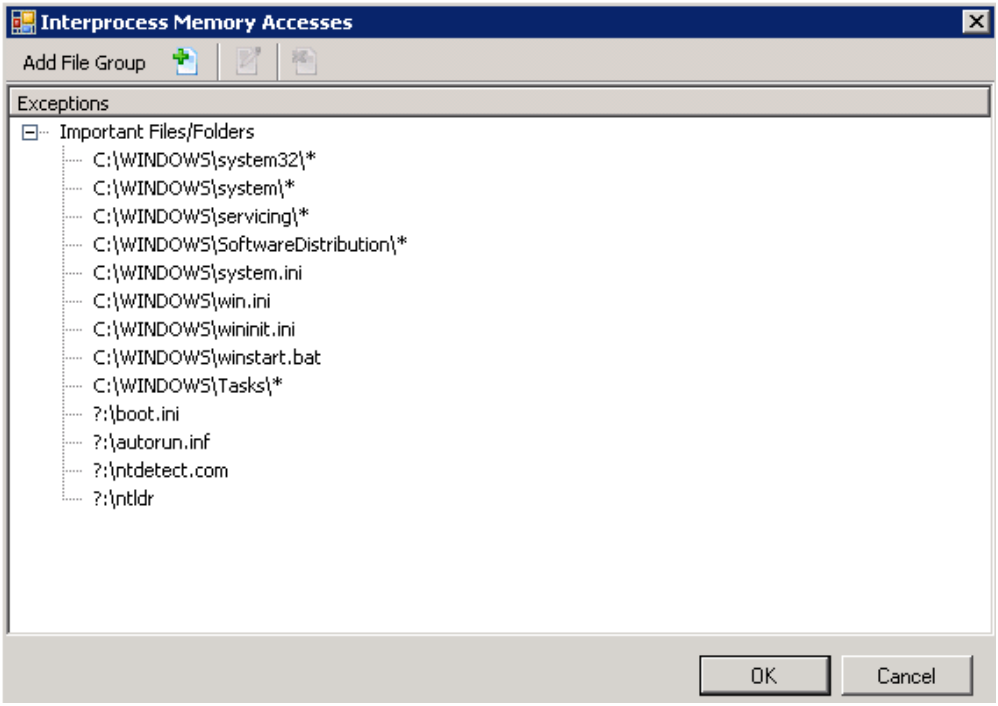
- Select the required file group and click the icon. The 'Type Name of File Path' dialog box is displayed.

- Type the name of the file path in the format specified in the dialog box.
- Click **OK** to confirm. The name of the added file path is displayed in the main list under the selected file group.

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

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

- Select **Yes** to enable monitoring and protect the application or file group against the process listed in the **Protection Type** column. Select **No** to disable such protection.
- Click the **Modify** button to specify the policy exceptions. This opens the **Interprocess Memory Accesses** dialog box.



- **Click here** for the step by step process of adding file groups and files.

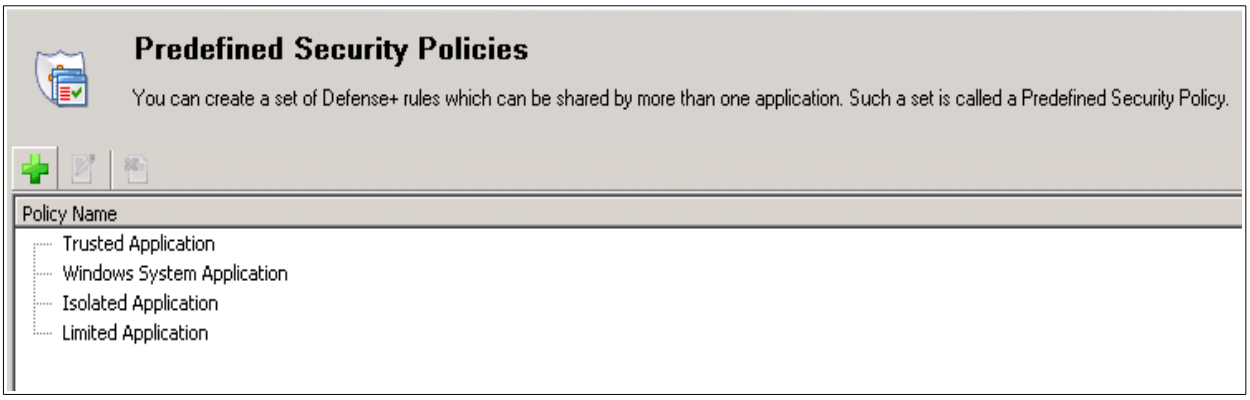
4.2.2.5. Predefined Security Policies

As the name suggests, a Predefined Security Policy is a set of **access rights and protection settings** that have been saved and can be re-used and deployed on multiple applications. Each policy is comprised of a number of 'Rules' and each of these 'Rules' is defined by a set of conditions / settings / parameters. 'Predefined Security Policies' is a set of policies that concern an application's access rights to memory, other programs, the registry etc.

Note: This section is for advanced and experienced administrators. New and inexperienced administrators to Comodo Internet Security are advise to first read the **Computer Security Policy** section in this help guide.

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

- Click **Predefined Security Policies** in Defense+ > Advanced to open the Predefined Security Policies interface. There are four default security policies listed under the Policy Name column.



To view or edit an existing predefined policy

1. Select the Policy Name and click the icon.
2. Make the required changes and **OK** to confirm.

Note: It is possible to modify a policy's name and make changes to its **'Process Access Rights' and 'Protection Settings'** from this interface. Any changes made here is automatically rolled out to all applications currently under that policy.

To create a new predefined policy

1. Click the icon, type a name for the policy then follow the same configuration procedure as outlined for creating a custom, application specific policy. **Click here to view the procedure**. Once created, the policy is available for deployment onto specific application or file groups via the **Computer Security Policy** section of Defense+.

4.2.2.6. Image Execution and Control Settings

Image Execution Control is an integral part of the Defense+ engine. If the Defense+ Security Level is set to **'Train with Safe Mode' or 'Clean PC Mode'**, then it is responsible for authenticating every executable image that is loaded into the memory.

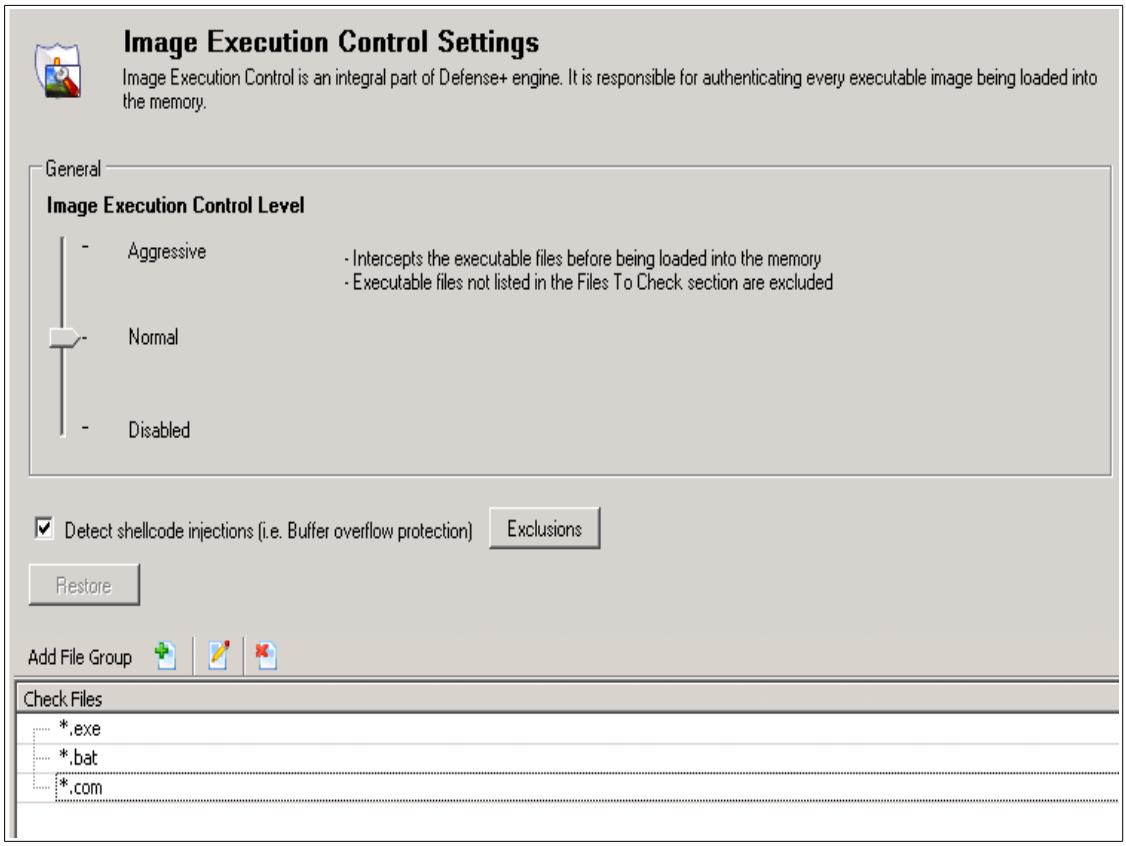
Comodo Internet Security calculates the hash of an executable at the point it attempts to load into memory. It then compares this hash with the list of known / recognized applications that are on the Comodo safe list. If the hash matches the one on record for the executable, then the application is safe. If no matching hash is found on the safelist, then the executable is 'unrecognized' and an alert is generated.

This area helps to quickly determine how proactive the monitor should be and which types of files it should check.

- Click **Image Execution Control Settings** in Defense+ > Advanced Task to open the Image Execution Control Settings interface.

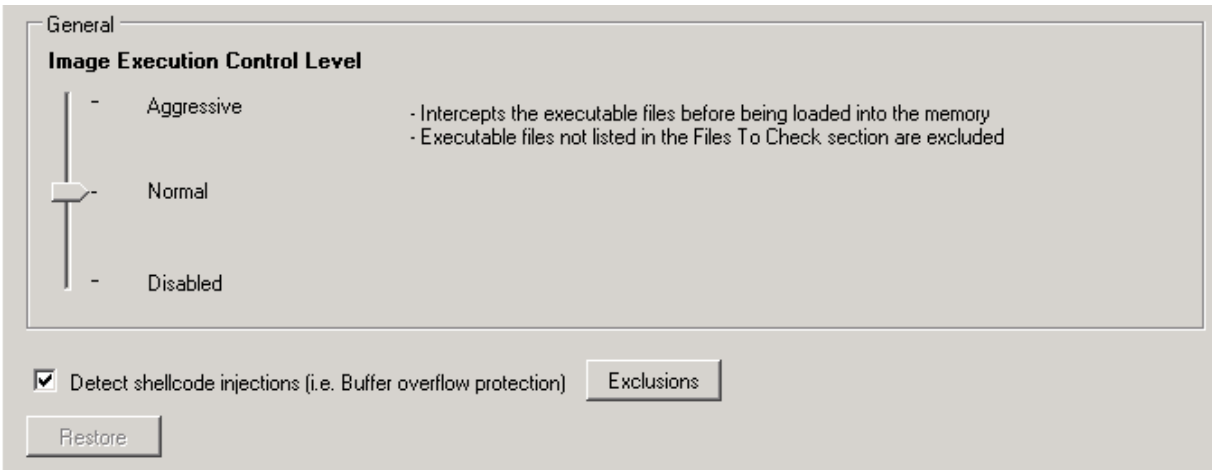
This setting is divided into two sections:

- **General Settings** section
- **Files to Check** section



General Settings

Slider Options



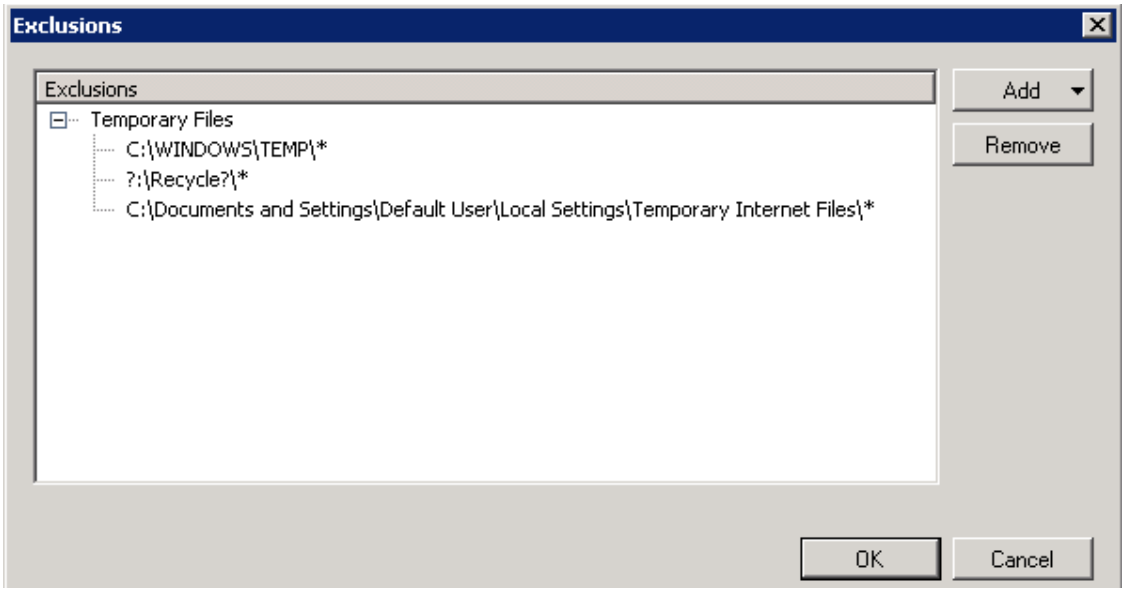
1. Adjust the slider to the preferred protection level. The description corresponding to the selected option is displayed in the right hand side of the options.
2. Detect Shellcode injections (i.e. Buffer overflow protection). Select this checkbox to turn-on Buffer over flow protection.

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

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

Comodo recommends that this setting to be maintained selected always.

3. Click the **Exclusion** button to exclude some of the file types from being monitored under **Detect Shellcode injections**. The following dialog box is displayed.



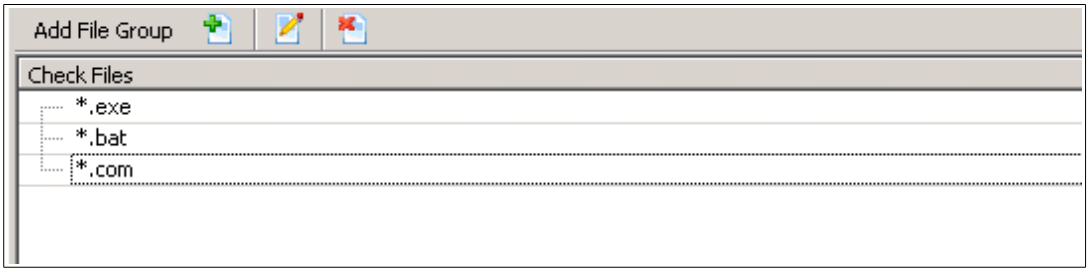
1. Click **Add** button and select File Groups option to include file groups to the Exclusions list.
2. Click **Remove** to remove selected entries from the exclusions list.

Note: These settings are recommended for advanced administrators only.

3. Click **OK** to confirm settings.

Files to Check

The **Files to Check** section displays the file types that Defense+ checks using the Image Execution Level specified in the **General** section.



Note: The default and recommended setting is *.exe, *.bat and *.com. This means every executable with those extensions are authenticated by Defense+ before it is allowed to run. If Defense+ is unable to authenticate a particular file then an alert is received that asks permission before the application allowed to run.

1. Click the Add File Group button to add additional file groups to the 'Files to check' list.
2. Click **OK** to confirm the changes.

4.2.2.7. Defense+ Settings

The Defense+ component of Comodo Internet Security is a host intrusion prevention system that constantly monitors the activities of all executable files on a PC. With Defense+ activated, the administrator is warned EVERY time an unknown application executable (`.exe, .dll, .sys, .bat, etc`) attempts to run. The only executables that are allowed to run are the ones that the administrator gives permission to. An application can be given such permission to run in a variety of ways including; manually granting them execution rights in **Computer Security Policy**; by deciding to treat the executable as trusted at Defense+ alert or simply because the application is on the Comodo safe list. Defense+ also automatically protects system-critical files and folders such as registry entries to prevent unauthorized modification. Such protection adds another layer of defense to Comodo Internet Security by preventing malware from ever running and by preventing any processes from making changes to vital system files.

Note: This page is often referred to 'executables', the most recognizable of which is the .exe file. Other types of executable files include those with extensions .cpl .dll, .drv, .inf, .ocx, .pf, .scr, .sys.

The Defense+ Settings area allows to quickly configure the security level and behavior of Defense+ during operation.

- Click on **Defense+ Settings** in Defense+ > Advanced Tasks to open the Defense+ Settings interface.
- This settings is divided into two sections:
- **General Settings** section
- **Monitor Settings** section

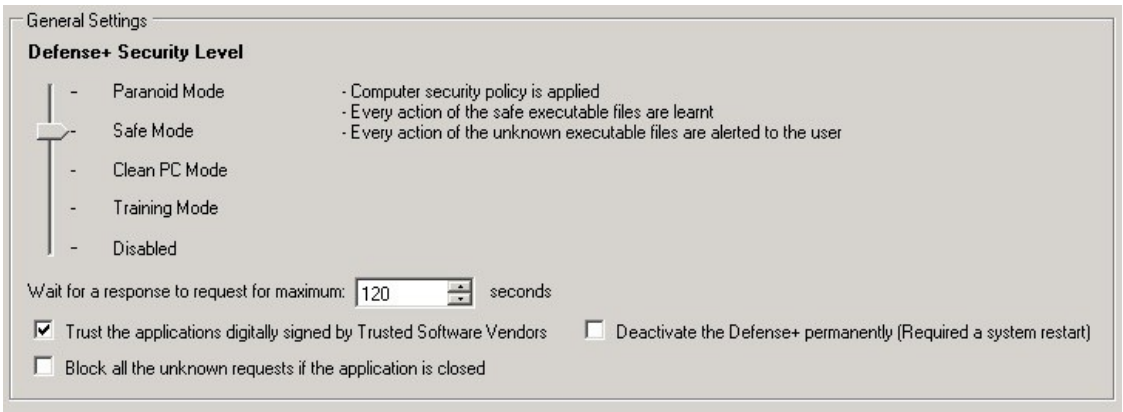
General Settings

The General Settings section allows to customize the behavior of Defense+ by adjusting the slider to switch between preset security levels.

Slider Options

Slider Options - General section	
Option	**Description**
Paranoid	This is the highest security level setting and means that Defense+ monitors and controls all executable files apart from those that have been deemed safe. Comodo Internet Security Configuration editor does not attempt to learn the behavior of any applications - even those applications on the Comodo safe list, and only uses the configuration settings to filter critical system activity. Similarly, the Comodo Internet Security

Slider Options - General section	
	Configuration editor does not automatically create 'Allow' rules for any executables - although there is still an option to treat an application as 'Trusted' at the Defense+ alert. Choosing this option generates the most amount of Defense+ alerts and is recommended for advanced administrators who require complete awareness of activity on their system.
Safe Mode	While monitoring critical system activity, Defense+ automatically learns the activity of executables and applications certified as 'Safe' by Comodo. It also automatically creates 'Allow' rules these activities. For non-certified, unknown, applications, an alert is received whenever that application attempts to run. If the application is chosen, it can be added to the safe list by choosing 'Treat this application as a Trusted Application' at the alert. This instructs Defense+ not to generate an alert the next time it runs. If the machine is not new or known to be free of malware and other threats as in 'Clean PC Mode' then Train with Safe Mode' is recommended setting - combining the highest levels of security with an easy-to-manage number of Defense+ alerts.
Clean PC Mode	From the time the slider is set to 'Clean PC Mode', Defense+ learn the activities of the applications currently installed on the computer while all new executables introduced to the system are monitored and controlled. This patent-pending mode of operation is the recommended option on a new computer or one that the administrator knows to be clean of malware and other threats. *From this point onwards* Defense+ alerts the administrator whenever a new, unrecognized application is being installed**.** In this mode, the files in 'My Pending Files' are excluded from being considered as clean and are monitored and controlled.
Training Mode	Defense+ monitors and learns the activity of any and all executables and creates automatic 'Allow' rules until the security level is adjusted. No Defense+ alerts are received in 'Training Mode'. 'Training Mode' setting should be chosen only if there is 100% surety that all applications and executables installed in the computer are safe to run. ***Tip***:This mode can be used as the "Gaming Mode". It is handy to use this setting temporarily while running an (unknown but trusted) application or Games for the first time. This suppresses all Defense+ alerts while Comodo Internet Security learns the components of the application that need to run on the machine and automatically create 'Allow' rules for them. (Later, the system can be switched back to 'Train with Safe Mode' mode).
Disabled	Disables Defense+ protection. All executables and applications are allowed to run irrespective of the configuration settings. Comodo strongly advise against this setting unless the administrator is confident that there is an alternative intrusion defense system installed on the computer.



1. Adjust the slider to the preferred protection level. The description corresponding to the selected option is displayed in the right hand side of the options.
2. Enter the duration or select the duration using the up / down button in the 'Wait for a response to request for maximum' filed to determine how long Comodo Internet Security shows a Defense+ alert without any administrator

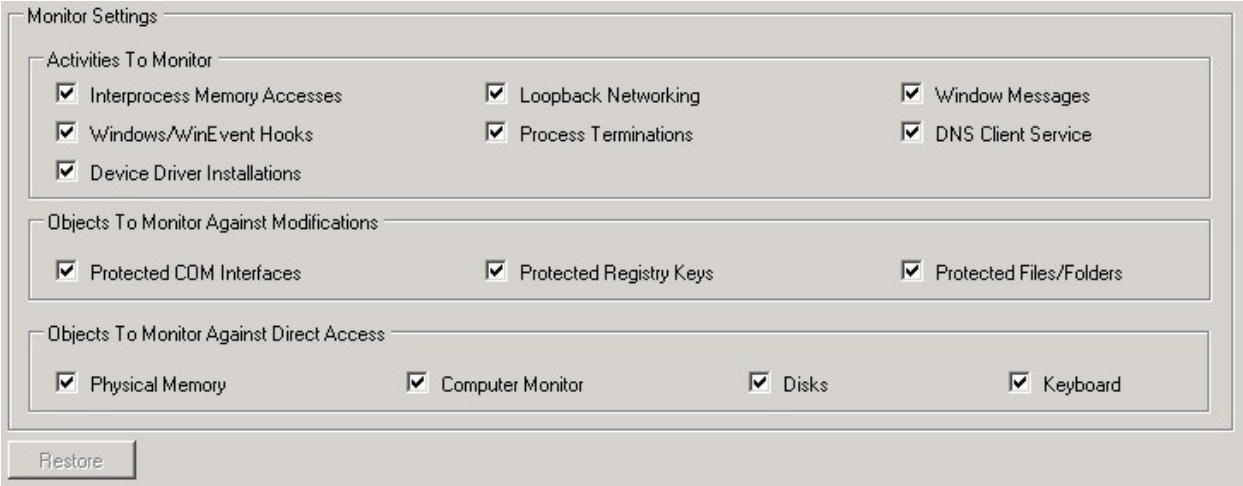
intervention. By default, it is set to 120 seconds.

3. Select the 'Trust the applications digitally signed by Trusted Software Vendors' checkbox to add softwares that are signed by a Trusted Certificate Authority to the safe list. Comodo recommend leaving this option enabled.
4. Select the 'Block all the unknown requests if the application is closed' checkbox to block all unknown requests (those not included in **Computer Security Policy**) if Comodo Internet Security is not running / has been shut down.
5. Select the 'Deactivate Defense+ permanently (Requires a system restart)' to shutdown the Defense+ Host Intrusion element of Comodo Internet Security PERMANENTLY. The firewall and antivirus are not affected and continues to protect the computer even if Defense+ is deactivated. Comodo does not recommend administrators to close Defense+ unless they are sure they have alternative Intrusion Prevention Systems installed.

Monitor Settings

The 'Monitor Settings' section allows configuration of activities, entities and objects that should be monitored by Defense+.

Note: The settings chosen here are universally applied. If monitoring of an activity, entity or object using this interface is disabled, then it completely switch off monitoring of that activity on a ***global*** basis - effectively creating a universal '**Allow**' rule for that activity. This 'Allow' setting ***over-rules*** any policy specific 'Block' or 'Ask' setting for that activity that has been selected using the '**Access Rights**' and '**Protection Settings**' interface.



Activities To Monitor

Checkbox options

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

Checkbox Options - Monitor Settings section - Activities to Monitor	
	of the mouse and keyboard to remotely administer the computer.
Device Driver Installations	Device drivers are small programs that allow applications and / or operating systems to interact with a hardware device on the computer. Hardware devices include disk drives, graphics card, wireless and LAN network cards, CPU, mouse, USB devices, monitor, DVD player etc. Even the installation of a perfectly well-intentioned device driver can lead to system instability if it conflicts with other drivers on the system. The installation of a malicious driver could, obviously, cause irreparable damage to the computer or even pass control of that device to a hacker.
Loopback Networking	Loopback connections refer to the internal communications within a PC. Any data transmitted by a computer through a loopback connection is immediately also received by it. This involves no connection outside the computer to the internet or a local network. Loopback channel attacks can be used to flood a computer with TCP and/or UDP requests which can smash the IP stack or crash the computer.
Process Terminations	A process is a running instance of a program. (For example, the Comodo Internet Security process is called 'cfp.exe'. Press 'Ctrl+Alt+Delete' and click on 'Processes' to see the full list that are running on a system). Terminating a process, obviously, terminate the program. Viruses and Trojan horses often try to shut down the processes of any security software has been running in order to bypass it.
Windows Messages	This setting means Comodo Internet Security monitors and detects if one application attempts to send special Windows Messages to modify the behavior of another application (e.g. by using the WM_PASTE command).
DNS Client Service	This setting gives an alert if an application attempts to access the 'Windows DNS service' - possibly in order to launch a DNS recursion attack. A DNS recursion attack is a type of Distributed Denial of Service attack whereby an malicious entity sends several thousand spoofed requests to a DNS server. The requests are spoofed in such a way that they appear to come from the target or 'victim' server but in fact can come from different sources - often a network of 'zombie' PC's which are sending out these requests without the owners knowledge. The DNS servers are tricked into sending all their replies to the victim server - overwhelming it with requests and causing it to crash. Note for beginners: DNS stands for Domain Name System. It is the part of the Internet infrastructure that translates a familiar domain name, such as 'example.com' to an IP address like 123.456.789.04. This is essential because the Internet routes messages to their destinations on the basis of this destination IP address, not the domain name. Whenever a domain name is typed, the Internet browser contacts a DNS server and makes a 'DNS Query'. In simplistic terms, this query is 'What is the IP address of example.com?'. Once the IP address has been located, the DNS server replies to the computer, telling it to connect to the IP in question.

1. Select the 'Interprocess Memory Access' checkbox to enable Defense+ to give alert when an application attempts to modify the memory space allocated to another application.
2. Select the 'Windows / WinEvent Hooks' checkbox to give a warning every time a hook is executed by an untrusted application.
3. Select the 'Device Driver Installations' checkbox to enable Defense+ to give alert every time a device driver is installed on the machine by an untrusted application.
4. Select 'Loopback Networking' checkbox to enable Defense+ to give alerts every time a process attempts to communicate using the loopback channel.
5. Select the 'Process Terminations' checkbox to enable Defense+ to monitor and alert for all attempts by an untrusted application to close down another application.
6. Select the 'Windows Messages' checkbox to monitor and detect if one application attempts to send special Windows Messages to modify the behavior of another application.

7. Select the 'DNS Client Service' checkbox to prevent malware from using the DNS Client Service to launch an attack.

Objects To Monitor Against Modifications

1. Select the 'Protected COM Interfaces' checkbox to enable the monitoring of COM interfaces specified **here**.
2. Select the 'Protected Registry Keys' checkbox to enable the monitoring of Registry keys specified **here**.
3. Select the 'Protected Files/Folders' checkbox to enable the monitoring of files and folders specified **here**.

Objects To Monitor Against Direct Access

Note: The options in this region determines whether or not Comodo Internet Security should monitor access to system critical objects in the computer. Using direct access methods, malicious applications can obtain data from a storage devices, modify or infect other executable software, record keystrokes and more. Comodo advises the administrator to leave these settings enabled.

Checkbox Options - Monitor Settings section - Objects to Monitor Against Direct Access	
Option	**Description**
Physical Memory	Monitors the computer's memory for direct access by applications and processes. Malicious programs attempt to access physical memory to run a wide range of exploits - the most famous being the 'Buffer Overflow' exploit. Buffer overruns occur when an interface designed to store a certain amount of data at a specific address in memory allows a malicious process to supply too much data to that address. This overwrites its internal structures and can be used by malware to force the system to execute its code.
Computer Monitor	Comodo Internet Security raises an alert every time a process tries to directly access the computer monitor. Although legitimate applications sometimes require this access, there is also an emerging category of spyware-programs that use such access to monitor the activities. (For example, to take screen shots of the current desktop; to record browsing activities etc.)
Disks	Monitors the local disk drives for direct access by running processes. This helps guard against malicious software that need this access to, for example, obtain data stored on the drives, destroy files on a hard disk, format the drive or corrupt the file system by writing junk data.
Keyboard	Monitors the keyboard for access attempts. Malicious software, known as 'key loggers', can record every stroke made on the keyboard and can be used to steal passwords, credit card numbers and other personal data.

1. Select the 'Physical Memory' checkbox to monitor the computer's memory and to raise an alert every time an application attempts to establish direct access to the memory.
2. Select the 'Computer Monitor' checkbox to monitor and to raise an alert every time an application attempts to establish direct access to the computer monitor.
3. Select the 'Disks' checkbox to monitor the local disk drives and to raise an alert every time an application attempts to establish direct access to the drives.
4. Select the 'Keyboard' checkbox to monitor the keyboard and to raise an alert every time an application attempts to establish direct access to the keyboard.

4.3. Antivirus Overview

The Antivirus center allows to quickly and easily configure all aspects of the Antivirus component of Comodo Internet Security (hereafter known simply as 'Comodo Antivirus').

Comodo Antivirus leverages multiple technologies, including Real-time / On-Access Scanning and Manual / On Demand Scanning and to immediately start cleaning or quarantining suspicious files from the hard drives, shared disks, emails,

downloads and system memory. The interface also allows administrator to create custom scan profiles which can be re-used across all scan types and features full event logging, quarantine and file submission facilities. Comodo Antivirus detects and removes threats that are present in the machine and forms an additional layer of security on top of the threat prevention offered by the Firewall and Defense+ components. The heuristics scanning capability of the application identifies previously unknown viruses and Trojans.

In order to maintain maximum security levels, Comodo advises administrators to run regular Antivirus scans.

On-Demand scanning is also seamlessly integrated into the Windows operating system. Administrators can scan specific objects 'on the fly' by simply right-clicking on a file, folder or drive and selecting **Scan with Comodo AntiVirus** from the context sensitive menu.

The Antivirus center can be accessed at all times by clicking on the Antivirus Shield button 

Comodo Antivirus section is divided into the Virus Scanner area and Exclusions area. Click the links below to see detailed explanations of each area in this section.

- **Virus Scanner**
- **Exclusions**

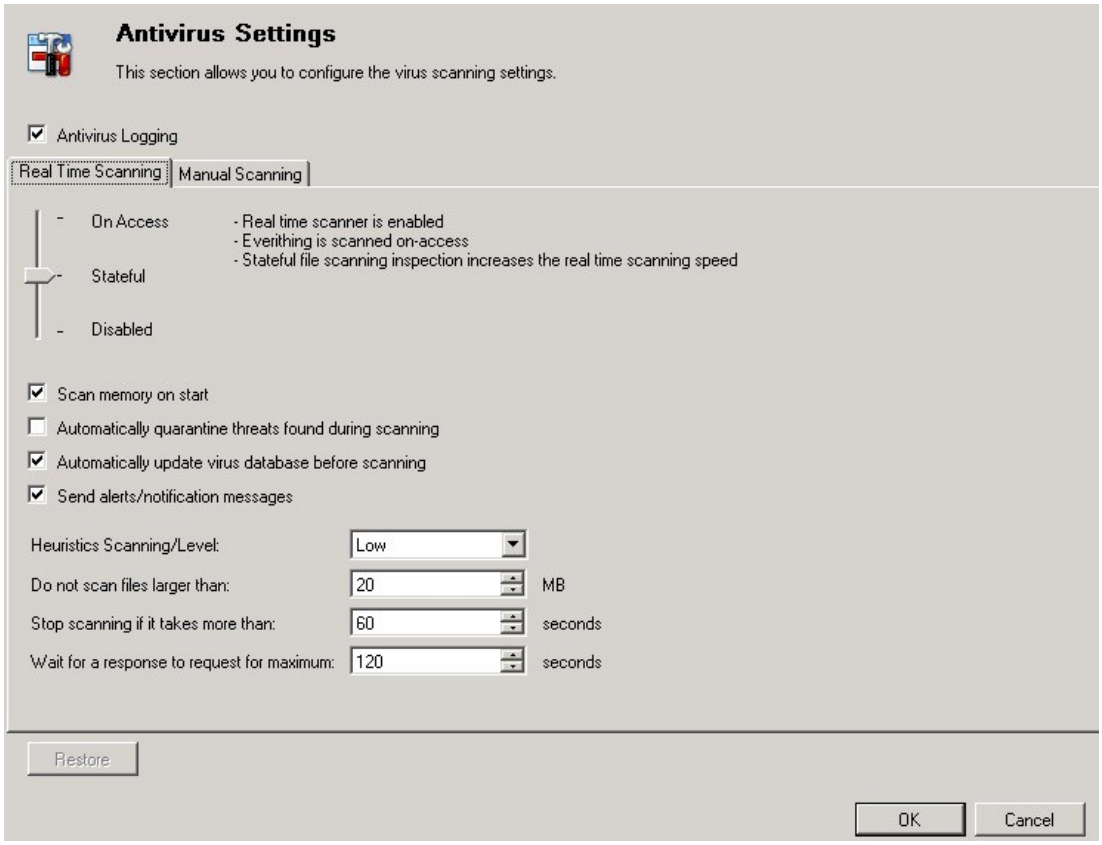
4.3.1. Virus Scanner

The Antivirus Settings configuration interface allows to customize options related to Real Time Scanning (On-Access Scanning) and Manual Scanning. The settings made for each type of the scan applies to all future scans of that type.

- Click on **Virus Scanner** in Antivirus to open the Antivirus Settings interface.

This setting has two tabs:

- **Real Time Scanning** tab
- **Manual Scanning** tab



Real Time Scanning

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

The Real Time Scanner also scans the system memory on start. If a program or file which creates destructive anomalies is launched, then the scanner blocks it and send an alert immediately - giving real time protection against threats.

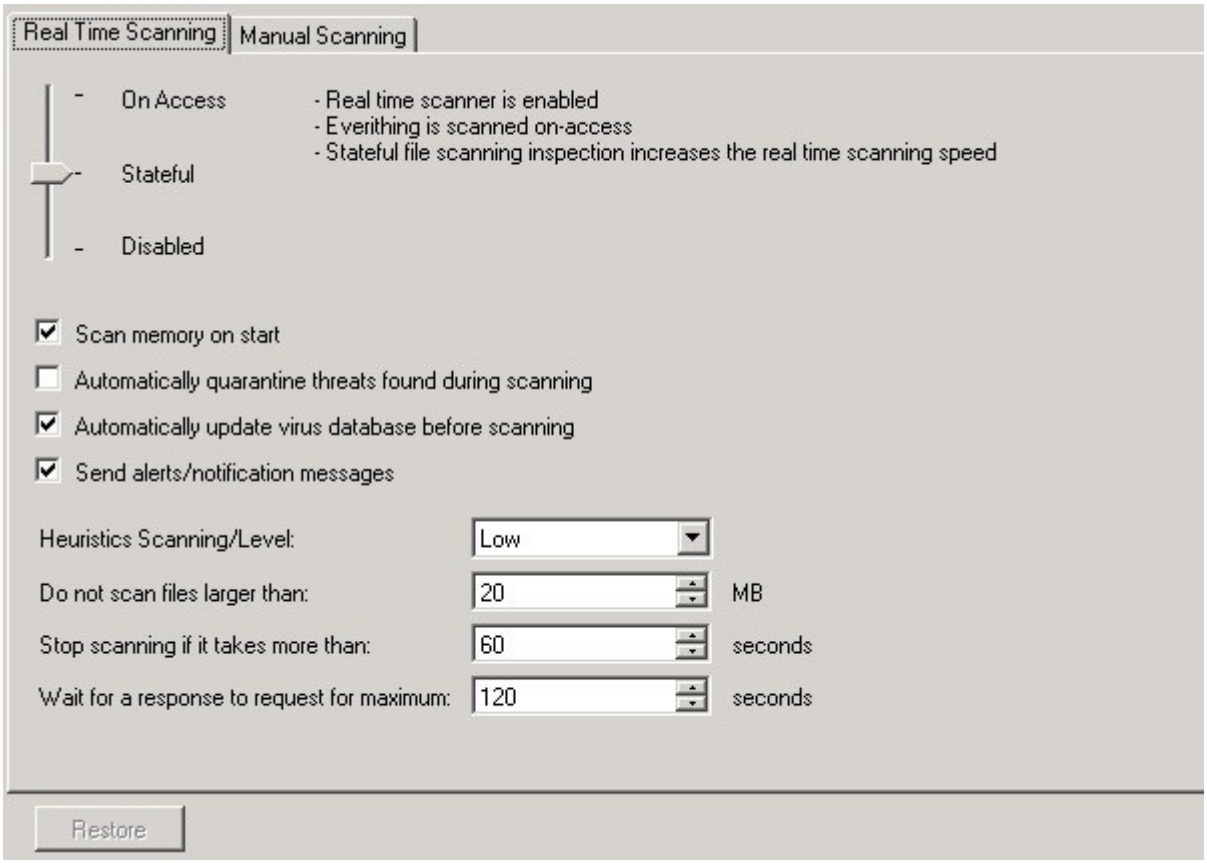
Options to automatically remove the threats found during scanning and to update virus database before scanning is also available. It is highly recommended that Real Time Scanner is enabled to ensure that the system remains continually free of infection.

The Real Time Scanning setting allows to switch the On Access scanning between **Disabled**, **Stateful** and **On Access** and allows to specify detection settings and other parameters that are deployed during on-access scans.

Slider Options

Slider Options - Real Time Scanning tab	
Option	**Description**
On Access	Provides the highest level of On Access Scanning and protection. Any file opened is scanned before it is run and the threats are detected before they are getting a chance to be executed.
Stateful	Stateful File Inspection (tm) feature is for real time virus scanning to minimize the effects of on-access scanning on the system performance. Selecting the 'Stateful' option means CIS scans only files that have not been scanned since the last virus update - greatly improving the speed, relevancy and effectiveness of the scanning.

Disabled	Disables Real time scanning. Antivirus does not perform any scanning and the threats cannot be detected before they impart any harm to the system



1. Adjust the slider to the preferred level. The description corresponding to the selected option is displayed in the right hand side of the options.
2. Select the **'Scan memory on start'** check box to enable the Antivirus to scans the system memory during system start-up.
3. Select the **'Automatically quarantine threats found during scanning'** check box enable the Antivirus to move the file detected to be containing the malware, to Quarantined Items. From the quarantined items the files can be restored or deleted as required.
4. Select the **'Automatically update virus database before scanning'** check box to enable Antivirus to check for latest virus database updates from Comodo website and downloads the updates automatically on system start-up and subsequently at regular intervals.
5. Select the **'Send alerts / notification messages'** check box to show alerts whenever virus is discovered in the system.

Note: Alerts are the pop-up notifications that appear in the lower right hand side of the screen whenever the on-access scanner discovers a virus in the system. These alerts are a valuable source of real-time information that helps the administrator to immediately identify which particular files are infected or are causing problems. Disabling alerts does not affect the scanning process itself and it still continues to identify and deal with threats in the background.

6. Select the appropriate Heuristics Scanning / Level from the dropdown.

Note: Comodo AntiVirus 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 *typical* of a virus. If it is found to do so then the application deletes the file or recommend it for quarantine. Heuristics is about detecting *virus-like behavior or attributes* rather than looking for a precise virus signature that matches a signature on the virus blacklist.

This is a quantum leap in the battle against malicious scripts and programs as it allows the engine to 'predict' the existence of

new viruses - even if it is not contained in the current virus database.

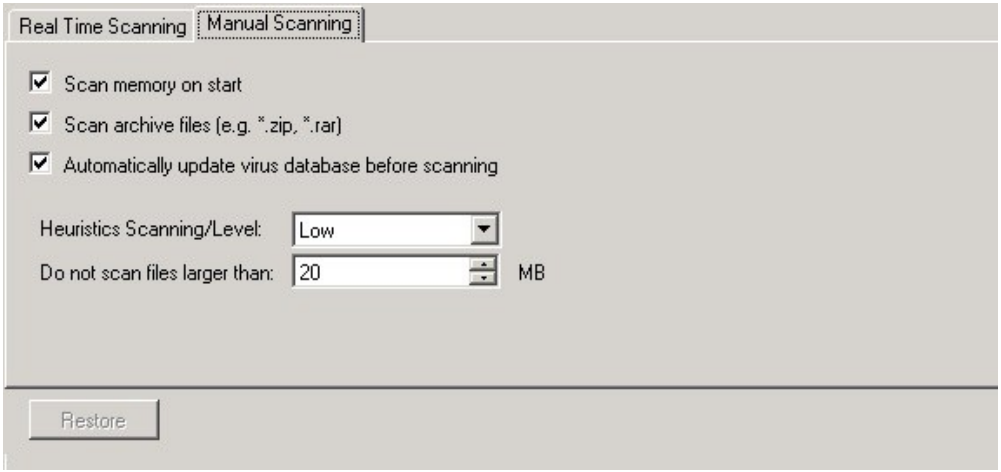
The drop-down menu allows to select the level of Heuristic scanning from the four levels:

- **Off** - Selecting this option disables heuristic scanning. This means that virus scans only use the 'traditional' virus signature database to determine whether a file is malicious or not.
- **Low** - Lower sensitivity to detecting unknown threats but the possibility of false positives is less.
- **Medium** - Detects unknown threats with medium sensitivity but the possibility of false positives is also medium.
- **High** - Higher sensitivity to detecting unknown threats but this also raises the possibility of more false positives too.

7. Set the maximum size for scanning individual files during on-access scan using the up / down buttons in the **'Do not scan files larger than'** field.
8. Set the maximum time limit for scanning individual files during on-access scan using the up / down buttons in the **'Stop scanning if it takes more than'** field.
9. Set the time period for which the alert message should stay on the screen using the up / down buttons in the **'Keep an alert on the screen for'** field.

Manual Scanning

The Manual Scanning setting allows to set the properties and parameters for on demand scan.



1. Select the **'Scan memory on start'** checkbox to enable the Antivirus to scan the system memory while starting a manual scan.
2. Select the **'Scan archive files'** check box to enable the Antivirus to scan archive files such as .ZIP and .RAR files. An alert is displayed in compressed files for the presence of virus even before it is opened. These include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives.
3. Select the **'Automatically update virus database before scanning'** check box to enable Antivirus to checks for latest virus database updates from Comodo website and downloads the updates manually.
4. Select the appropriate Heuristics Scanning / Level from the dropdown.

Note: Comodo AntiVirus 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 *typical* of a virus. If it is found to do so then the application deletes the file or recommend it for quarantine. Heuristics is about detecting *virus-like behavior or attributes* rather than looking for a precise virus signature that matches a signature on the virus blacklist.This is a quantum leap in the battle against malicious scripts and programs as it allows the engine to 'predict' the existence of new viruses - even if it is not contained in the current virus database.The drop-down menu allows to select the level of Heuristic scanning from the four levels:

Off - Selecting this option disables heuristic scanning. This means that virus scans only use the 'traditional' virus signature database to determine whether a file is malicious or not.

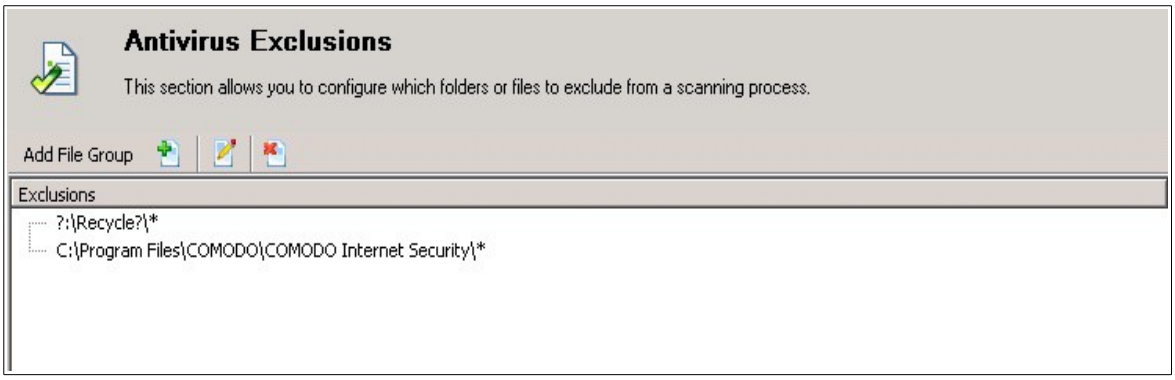
Low - Lower sensitivity to detecting unknown threats but the possibility of false positives is less.
Medium - Detects unknown threats with medium sensitivity but the possibility of false positives is also medium.
High - Higher sensitivity to detecting unknown threats but this also raises the possibility of more false positives too.

5. Set the maximum size for scanning individual files during manual scan using the up / down buttons in the **'Do not scan files larger than'** field.

4.3.2. Exclusions

The Exclusions interface displays a list of applications / files that are considered safe and ignored the alert during a virus scan. It is possible to manually add trusted applications and files that are to be excluded from virus scan through this interface. All items listed and all items added to the 'Exclusions' list are excluded from all future scans of all types.

- Click on **Exclusion** in Antivirus to open the Antivirus Exclusions interface.



To add an existing File Group as trusted and to be excluded from scanning

1. Click the Add File Group button to display the list of existing file groups. **Click here** for a description of the choices available when selecting a file.

2. Select the required File Group from the list. The selected File Group is displayed in the 'Exclusion' list.

To add a File to a file group

1. Select the required file group and click the icon. The 'Type Name of File Path' dialog box is displayed.

2. Type the name of the file path in the format specified in the dialog box.
3. Click **OK** to confirm. The name of the added file path is displayed in the main list under the selected file group.

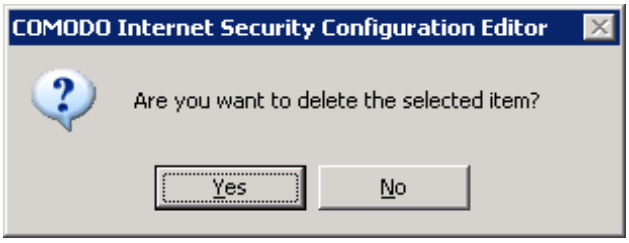
Note: To know how to create a new File Group and add a list of files to it, **Click here**.

To edit a File Group / File

1. Select the required File Group / File and click the icon. The corresponding dialog box is opened.
2. Make the necessary changes and click OK to confirm the changes.

To delete a File Group / File

1. Select the required File Group / File and click the icon. The following confirmation dialog box is displayed.



2. Click **Yes** to delete the selected item.

4.4. Common

The **Common** module section helps to create File Groups, Registry Keys and COM Groups, the entities of which are called in several interfaces within CIS Configuration Editor.

Click on the links below for detailed explanations of each area in this section.

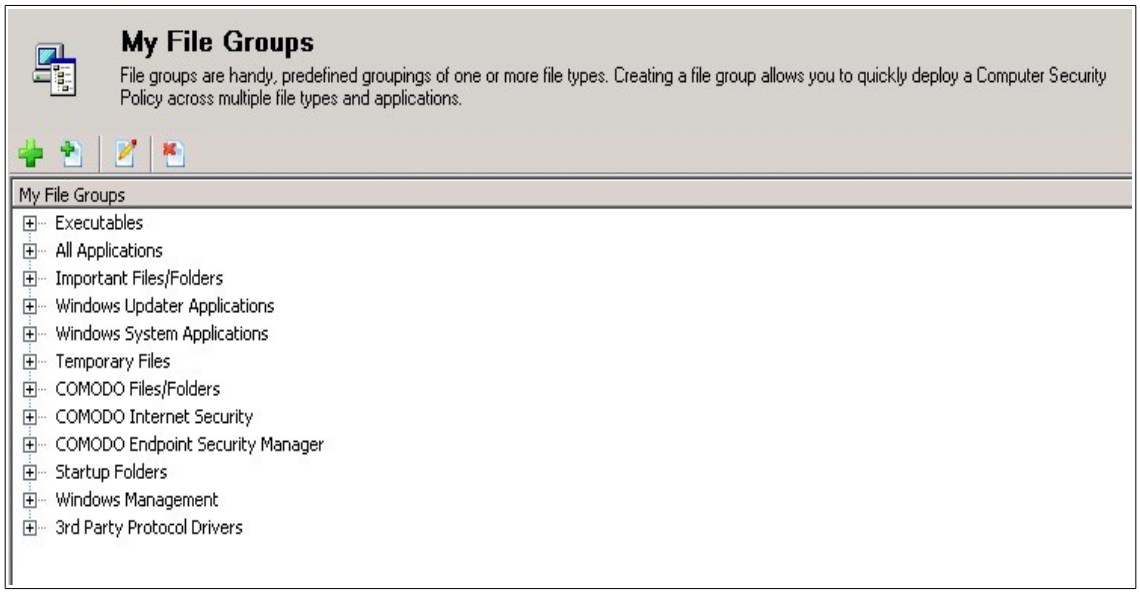
- **File Groups**
- **Registry Keys**

- **COM Groups**

4.4.1. File Groups

The **My File Groups** interface helps create predefined groups of one or more file types. Creating a file group allows to quickly deploy a Computer Security Policy across multiple file type and application.

- Click on **File Groups** in **Common** to open My File Groups interface.



Once opened, the 'My File Groups' window enables administrators to define new file groups and files, edit and delete file groups and files.

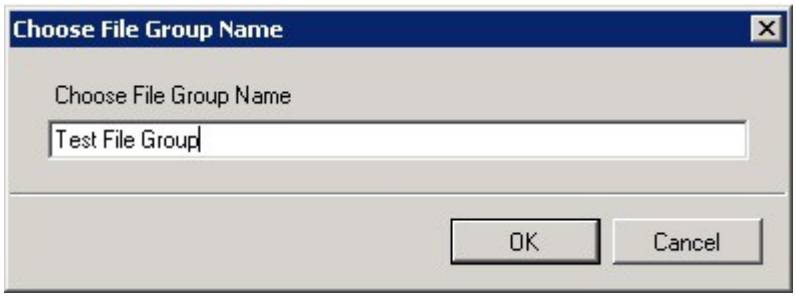
Window Specific Controls - My File Groups		
Menu Element	**Element Icon**	**Description**
Add New Group		Enables the administrator to add a New File Group
Add New File		Enables the administrator to add a single file to the selected File Group
Edit		Enables the administrator to edit the selected File Group / File
Remove		Removes the selected File Group / File

To create a new File Group

- Define a name for the File Group.
- Select the Files that needs to be added to this named group.

To define a name for the File Group

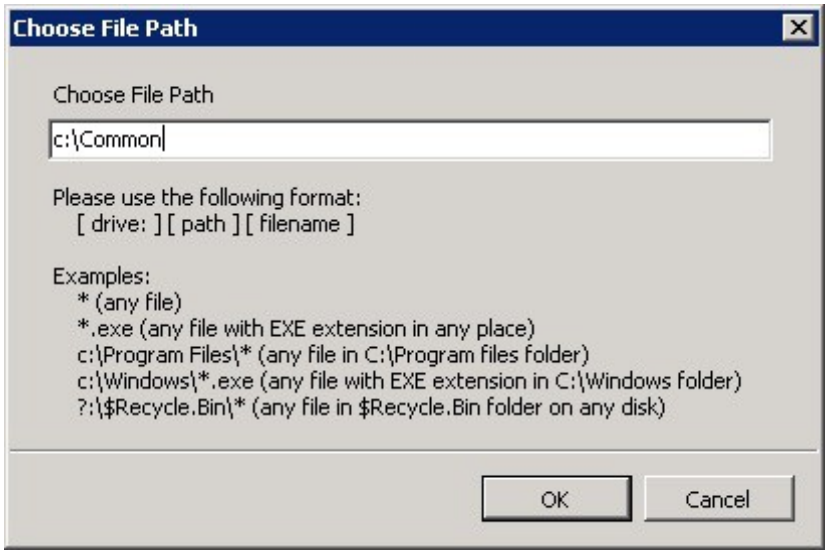
1. Click the icon in the 'My File Groups' window. The naming dialog box is displayed.



2. Type a name for the file group. In the image above, *Test File Group* is taken as an example.
3. Click **OK** to confirm the name. The name of the new file group is added to the My File Groups list:

To define Files for the File Group

1. Select the File Group for which the files are defined and click the icon in 'My File Groups' window. The 'Choose File Path' dialog box is displayed.



2. Type the name of the file path in the format specified in the dialog box.
3. Click **OK** to confirm. The name of the added file path is displayed in the main list under the selected file group.

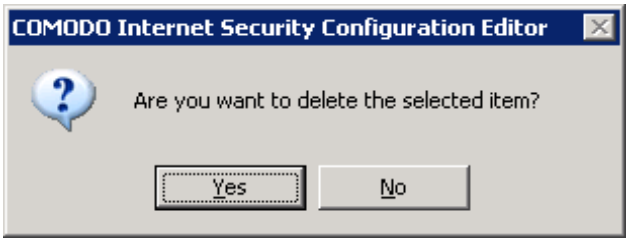
Note: To add more files to this File Group or to an existing File Group, select the appropriate File Group and repeat the process from the fourth step.

To edit a File Group / File

1. Select the required File Group / File and click the icon. The corresponding dialog box is opened.
2. Make the necessary changes and click **OK** to confirm the changes.

To delete a File Group / File

1. Select the required File Group / File and click the icon. The following confirmation dialog box is displayed.

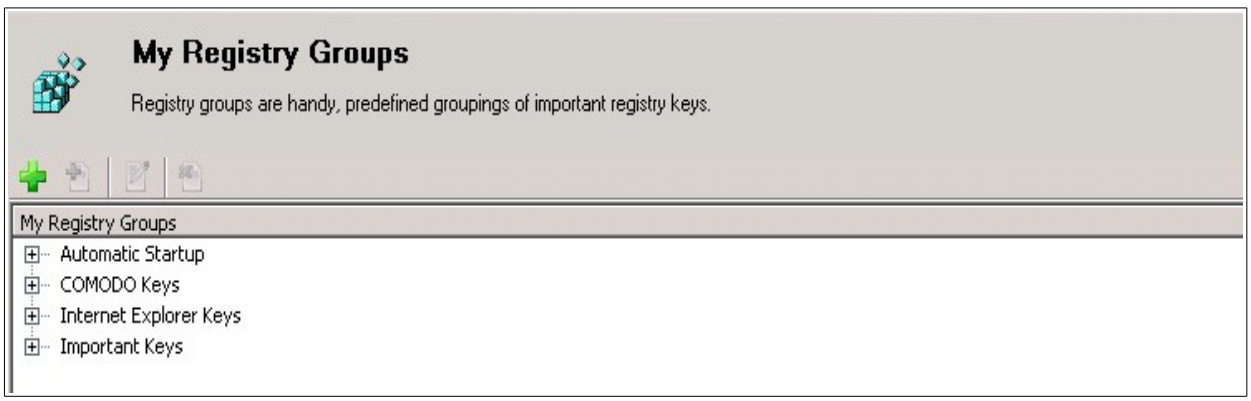


2. Click **Yes** to delete the selected item.

4.4.2. Registry Keys

The My Registry Groups interface helps create predefined groupings of important registry keys.

- Click on **Registry Keys** in **Common** to open My Registry Groups interface.



Once opened, the 'My Registry Groups' window enables administrators to define new registry groups and registry keys, edit and delete registry groups and registry keys.

Window Specific Controls - My Registry Groups		
Menu Element	**Element Icon**	**Description**
Add New Group		Enables the administrator to add a New Registry Group
Add New Entry		Enables the administrator to add a single entry to the selected Registry Group
Edit		Enables the administrator to edit the selected Registry Group / File path
Remove		Removes the selected Registry Group / File path

To create a new Registry Group

- Define a name for the Registry Group.
- Select the Registry Keys that needs to be added to this named group.

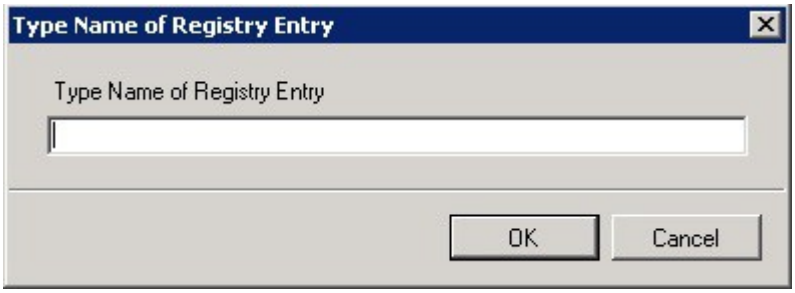
To define a name for the Registry Group

1. Click the  icon in the 'My Registry Group' window. The naming dialog box is displayed.

2. Type a name for the Registry Group. In the image above, *Test Registry Group* is taken as an example.
3. Click **OK** to confirm the name. The name of the new Registry Group is added to the Port Set list:

To add a Registry Key to a Registry group

1. Select the required Registry group and click the  icon. The 'Type Name of Registry Entry' dialog box is displayed.



2. Type the name of the Registry Entry.
3. Click **OK** to confirm. The name of the new registry key is displayed in the main list under the selected registry group.

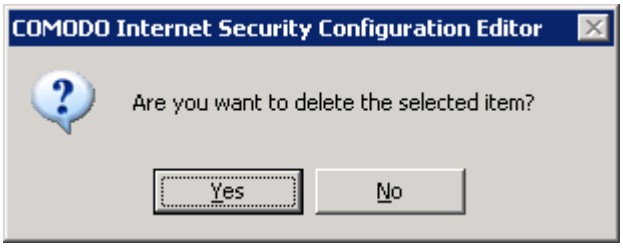
Note: To add more keys to this Registry Group or to an existing Registry Group, select the appropriate Registry Group and repeat the process from the fourth step.

To edit a Registry Group / Entry

1. Select the required Registry Group / Entry and click the icon. The corresponding dialog box is opened.
2. Make the necessary changes and click **OK** to confirm the changes.

To delete a Registry Group

1. Select the required Registry Group and click the icon. The following confirmation dialog box is displayed.



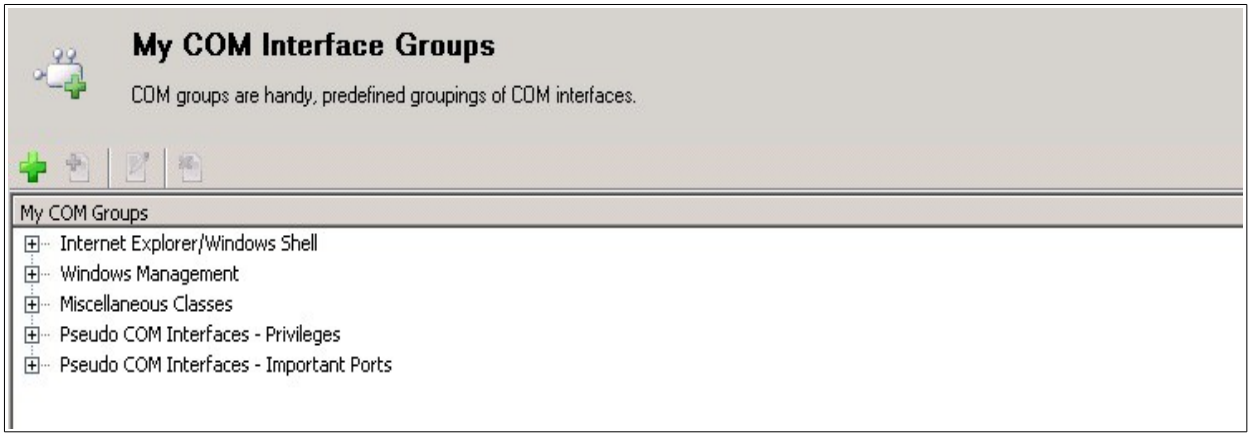
2. Click **Yes** to delete the selected item.

4.4.3. COM Groups

The My COM Interface Groups interface helps create predefined groupings of COM Interface.

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

- Click on **COM Groups** in Common to open My COM Interface Groups interface.



Once opened, the 'My COM Interface Groups' window enables administrators to define new COM interface groups, edit and

delete COM interface groups and files path.

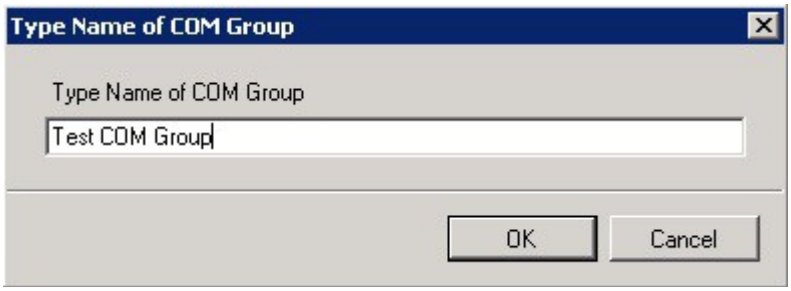
Window Specific Controls - My COM interface Groups		
Menu Element	**Element Icon**	**Description**
Add New Group		Enables the administrator to add a New COM interface Group
Add New GUID		Enables the administrator to add a file path to the selected COM interface Group
Edit		Enables the administrator to edit the selected COM interface Group / File path
Remove		Removes the selected COM interface Group / File path

To create a new COM Interface Group

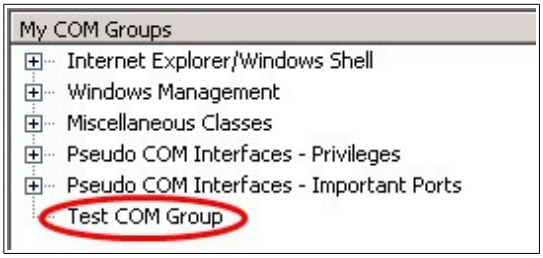
- Define a name for the COM Group.
- Select the File path that needs to be added to this named group.

To define a name for the COM Group

1. Click the icon in the 'My COM interface Groups' window. The naming dialog box is displayed.

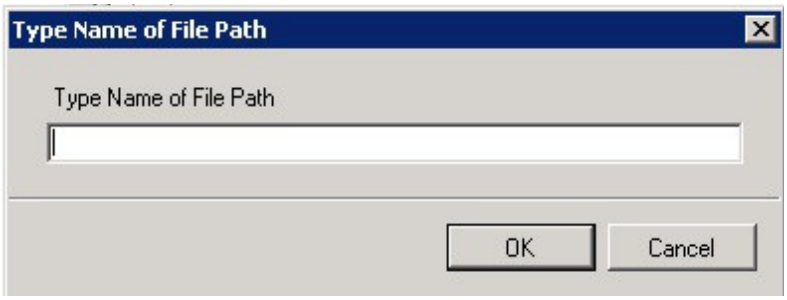


2. Type a name for the COM group. In the image above, *Test COM Group* is taken as an example.
3. Click **OK** to confirm the name. The name of the new COM group is added to the My COM Groups list.



To add a File Path to the a COM group

1. Select the required COM group and click the icon. The 'Type Name of File Path' dialog box is displayed.



2. Type the name of the File Path.
3. Click **OK** to confirm. The name of the new file path is displayed in the main list under the selected COM group.

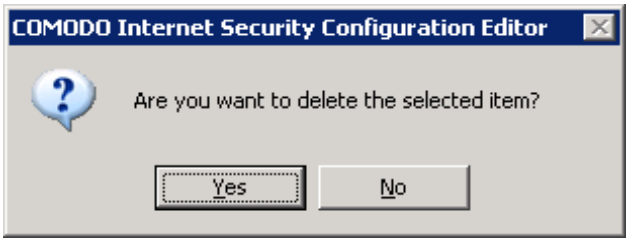
Note: To add more file paths to this COM Group or to an existing COM Group, select the appropriate COM Group and repeat the process from the fourth step.

To edit a COM Group / File path

1. Select the required COM Group / File path and click the icon. The corresponding dialog box is opened.
2. Make the necessary changes and click **OK** to confirm the changes.

To delete a COM Group / File path

1. Select the required COM Group / File path and click the icon. The following confirmation dialog box is displayed.



2. Click **Yes** to delete the selected item.

4.5. Miscellaneous Overview

The **Miscellaneous** section contains settings relating to overall configuration as well as handy utilities and shortcuts to help enhance and improve the experience with Comodo Internet Security.

It can be accessed at all times by clicking on the **Miscellaneous** button

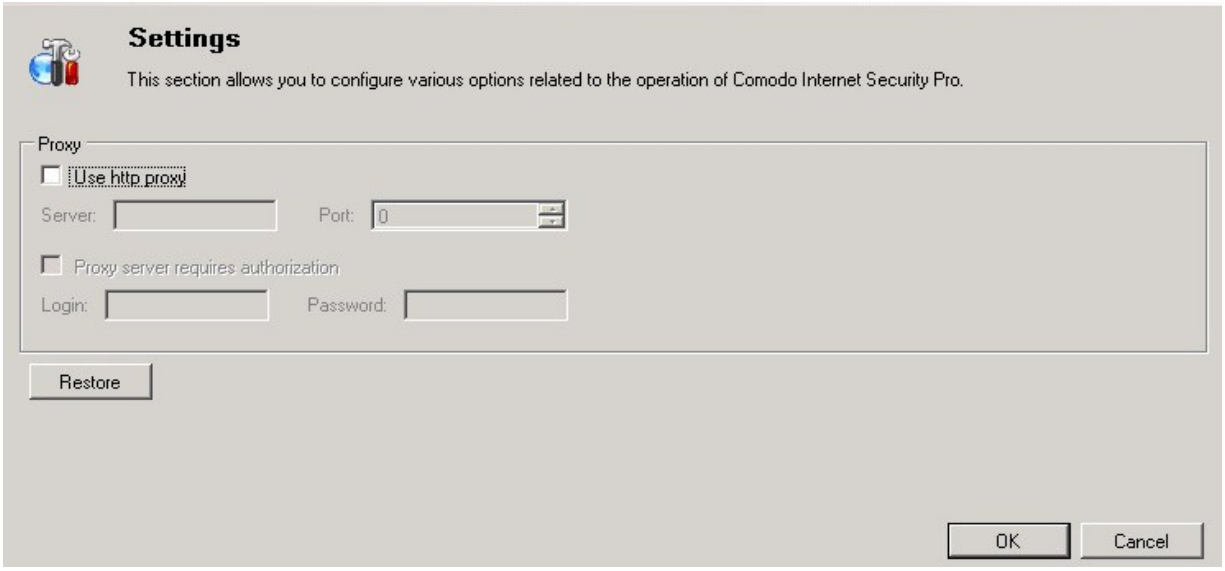
Click the link below to see detailed explanations of Settings section.

- **Settings**

4.5.1. Settings

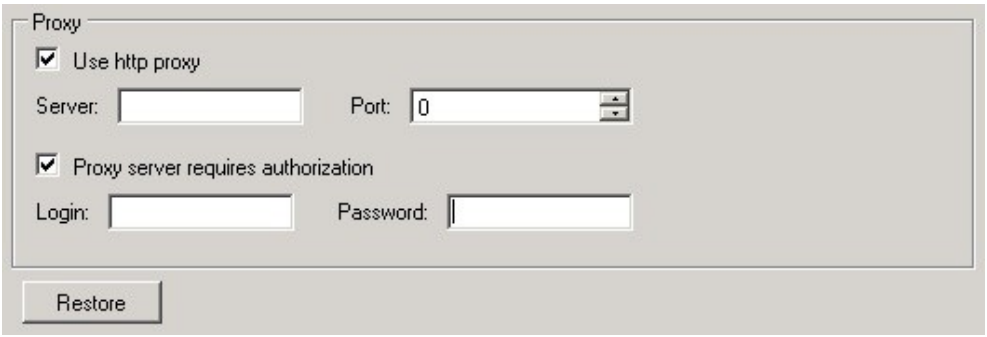
The **Settings** menu in Miscellaneous section allows the administrator to configure connectivity settings to Comodo servers for receiving Threatcast ratings, program updates etc. If a Proxy server is used in the network and if connectivity has to be established to that Proxy server, then the Proxy settings can be configured through this interface.

- Click on **Settings** in **Miscellaneous** to open the Settings interface.



1. Select the 'Use http proxy' checkbox to use the Proxy Server.

Note: Selecting the **Use http proxy** option enables the 'Server', 'Port' and 'Proxy server requires authorization' fields.



2. Enter the proxy server IP address or name in the 'Server' field.
3. Enter the port number or select the port number using the up / down button in the 'Port' field.
4. Select the 'Proxy server requires authorization' checkbox if the proxy server needs an authentication.

Note: Selecting the **Proxy server requires authorization** option enables the 'Log in' and 'Password' fields.

5. Enter the Log in ID for authorizing the proxy server in the 'Log in' field.
6. Enter the password for the Log in ID in the 'Password' field.

About Comodo

The Comodo companies are leading global providers of Security, Identity and Trust Assurance services on the Internet. Comodo CA offers a comprehensive array of PKI Digital Certificates and Management Services, Identity and Content Authentication (Two-Factor - Multi-Factor) software, and Network Vulnerability Scanning and PCI compliance solutions. In addition, with over 10,000,000 installations of its threat prevention products, Comodo Security Solutions maintains an extensive suite of endpoint security software and services for businesses and consumers.

Continual innovation, a core competence in PKI and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies as vital players in the Internet's ongoing development. Comodo, with offices in the US, UK, China, India, Romania and the Ukraine, secures and authenticates the online transactions and communications for over 200,000 business customers and millions of consumers, providing the intelligent security, authentication and assurance services necessary for trust in on-line transactions.

Security Solutions Inc.

1255 Broad Street

STE 100

Clifton, NJ 07013

United States

Tel: +1.888.256.2608

Tel: +1.703.637.9361

Email: **EnterpriseSolutions@Comodo.com**

For additional information on Comodo - visit **http://www.comodo.com**.