C·O·M·O·D·O

Creating Trust Online™

Comodo Firewall Pro 2.4

User Guide

CONTENTS

Getting Started

Firewall Basics

►*What is a Firewall?*

Broadly speaking, a computer firewall is a software program that prevents unauthorized access to or from a private network. Firewalls are tools that can be used to enhance the security of computers connected to a network, such as LAN or the Internet. They are an integral part of a comprehensive security framework for your network.

A firewall absolutely isolates your computer from the Internet using a "wall of code" that inspects each individual "packet" of data as it arrives at either side of the firewall — inbound to or outbound from your computer — to determine whether it should be allowed to pass or be blocked.

Firewalls have the ability to further enhance security by enabling granular control over what types of system functions and processes have access to networking resources. These firewalls can use various types of signatures and host conditions to allow or deny traffic. Although they sound complex, firewalls are relatively easy to install, setup and operate.

►*Why do I need one?*

As the Internet has come to play a role in the home and business alike, protection from unauthorized Internet users is a necessity. When your network is connected to a public network, it is exposed to spies, thieves, hackers, thrill seekers, and various other threats. Internet users need to be increasingly vigilant of security issues, as network traffic coming into the computer can cause damage to files and programs even when the user is away from the computer and the computer is idle. In a system that is not protected with any security measures, malicious code such as viruses can infect systems and cause damage that may be difficult to repair. The loss of financial records, e-mail, customer files, can be devastating to a business or to an individual.

What's New in Comodo Firewall Pro

New in Version 2.4.16

NEW! Multilanguage capabilities. Releasing version 2.4 with following 13 languages:

1) Chinese (Traditional)
2) Chinese (Simplified)
3) Dutch
4) French
5) Greek
6) Hungarian
7) Portugese (Brazilian)
8) Portugese (Continental)
9) Russian
10) Spanish (LA)
11) Spanish (Spain)
12) Swedish
13) Turkish

NEW! Activity->Connections sections shows per connection bytes in/out

NEW! Firewall icon shows animation as per incoming/outgoing traffic in system tray

FIXED! At times certain folder could remain locked when using firewall

FIXED! The bug causing SHA1 replies to be forgotten

FIXED! Few BSODs reported via forums and support

IMPROVED! Now firewall does not require user to activate license. It comes with lifetime free license on installation itself.

IMPROVED! Significantly improved self defense

a) Defense against automated windows messaging (Simulated mouse clicks)
b) File digital ceritificate verification for own binaries
c) Fixed DOS conditions in self defense handling
d) Fixed system driver crashes
e) Fixed some bugs that can cause priviledge escallation

IMPROVED! Improved OLE automation handling

IMPROVED! Fixed some minor bugs in tooltip texts

IMPROVED! Removed non-TCP/UDP application alerts until version 3.0

New in Version 2.3.6.81

FIXED! Network monitor rules were not loaded during system boot

FIXED! DHCP protocol stateful analysis were causing reconnection problems

FIXED! Comodo Firewall Pro no longer crashes when ShellExecute hooking software is installed (SuperAdblocker, counterspy etc.)

FIXED! Minor inaccuracies in tooltip text

FIXED! Log size is not remembered correctly

FIXED! Many other bugs are fixed according to the user bug reports

New in Version 2.3.5

NEW! Removed Comodo LaunchPad Installation

FIXED! Startup Delay if Terminal Services service is disabled

FIXED! Navigating between adapters using "Next" and "Previous" links could cause error message

FIXED! When no adapter active was showing wrong adapter information

New in Version 2.3.4

NEW! Reduced Memory Usage

NEW! Added Protocol Analysis Option

Protocol Analysis is key to the detection of fake packets used in denial of service attacks. This new feature means Comodo Firewall Pro checks every packet conforms to that protocols standards. If not, then the packets are blocked.

NEW! Added packet checksum verification feature

Every packet of data sent to your machine has a signature attached. Comodo Firewall Pro will recalculate the checksum of the target packet and compare this against the checksum stated in the signature. If the two do not match then Comodo Firewall Pro will block the packet. Altered checksums indicate that a packet has been altered since transmission.

NEW! Added an option to define Alert Frequency level

Users can now quickly configure the amount of alerts that Comodo Firewall Pro generates by raising or lowering a new slider.

NEW! Added defense for own registry keys and files against malware tampering

Meaning that Comodo Firewall Pro registry entries and files cannot be deleted or modified either accidentally or deliberately. This vital security feature prevents malicious programs or intruders from being able to shut down or sabotage your installation of Comodo Firewall Pro.

NEW! Added Suspicious file submission capability to popup alert

Each time Comodo Firewall Pro discovers unknown components within an application, the user is notified via an alert. In version 2.3, these particular alerts now contain a built in link to instantly submit the suspicious files to Comodo for analysis.

IMPROVED! Default network control rules

IMPROVED! New icons for rules section

IMPROVED! Tasks and Advanced section layouts are redesigned

IMPROVED! Effect on OS system performance has significantly been decreased

FIXED! Bug causing Windows to freeze (a rare but serious bug of BETA Releases)

FIXED! Bug causing Log Size selection to be forgotten after a reboot

FIXED! Bug causing legitimate packets to be dropped by protocol analysis

FIXED! The firewall will use the default browser instead of IE

REMOVED! Hardware details section from the summary section

New in Version 2.2.0

NEW! Skip advanced security checks

Skip advanced security checks options in the Application control rules is for the applications which user allows but still for some reasons they fail to connect.

NEW! CPF passes another leak test!!

Comodo Firewall Pro - passes one more leak test called BITS. (http://www.firewallleaktester.com/news.htm)

IMPROVED! Display Settings

Display issues seen in system's DPI setting higher than 96 DPI or while using large fonts settings for system has been fixed.

New in Version 2.1.0

NEW! Monitor COM/OLE Requests

Monitor COM/OLE requests" when enabled, forces CPF to detect any program hijacking attempt which may occur by misuse of COM/OLE interfaces by other programs.

NEW! Automatically Approve Safe Applications

Automatically approve safe applications option, when enabled, forces CPF to allow all activities of an application which is recognized as safe by its internal database of over 10000 applications. Unless explicitly blocked by a rule, Comodo Firewall Pro will allow any activity of the safe applications while still watching for suspicious activities. In case for an application action to be taken is set as 'Ask' and if it appears in safe database list of applications, it will be allowed without asking user. The firewall will still raise an alert if it detects anything suspicious. This option is useful for avoiding unnecessary number of questions.

IMPROVED! Zone Modification

A Machine or network can be represented as a zone to which a access can be granted or denied by specifying it in Application / Network rules. The newly designed easy to use GUI in Comodo Firewall Pro 2 allows the user to Add/Edit/Remove Zones.

New in Version 2.0.0

NEW! Application Component Authentication

Comodo Firewall Pro now validates all the components of an application before allowing it Internet access. These components can be dynamic link libraries, activex components that an application is using.

NEW! Application Behavior Analysis

Firewall Pro analyses each application's behavior and detects any suspicious activity before allowing internet access. This powerful new feature enables it to detect more trojan activity than any other firewall - including:

- DLL/Code injections
- Hidden Connection Attempts

NEW! Defense against Trojan Protocols

Comodo Firewall Pro now features advanced protocol driver level protection - essential for the defense of your PC against trojans having their own protocol drivers.

NEW! Smart Alerts

Alerts are completely redesigned in Comodo Firewall Pro. They are now simple and more intuitive. Every alert now includes a Security Considerations section which provides significant advices to users. Each alert also has an associated Security Risk level shown on the top of it to help users decide a course of action.

Although they are simple, the new alerts also have an option to be more verbose or simple. Basic popup logic removes unnecessary popup alerts whereas verbose logic reveals each activity to provide more details.

NEW! Windows Security Center Integration

Comodo Firewall Pro is now recognized by Windows XP SP2 Security Center as a trusted firewall and reports its state.

NEW! Self Protection against Termination of Critical Firewall Processes

A Trojan/Spyware/Virus may need to disable the firewall protection before performing its malicious operations. Comodo Firewall Pro secures itself to make sure its critical processes are always active and running.

NEW! PC Security during Booting

Comodo Firewall Pro 2 includes an option to secure the host while the operating system is booting. When enabled, it makes sure that no connections are established until booting process is completed.

NEW! Automatic Updater

Comodo Firewall Pro now includes an interactive automatic updater component so that users can check for updates any time.

NEW! Error Reporting Interface

To improve users' satisfaction, Comodo Firewall Pro 2 now includes an XP style bug reporting interface.

IMPROVED! Firewall Logging

The new logging structure in Comodo Firewall Pro is more powerful than before. It reveals all the activities with detailed descriptions of the events. It also allows exporting the logs in HTML format.

IMPROVED! Security Rules Interface

Comodo Firewall Pro 2 has a completely redesigned security rules interface. More powerful, flexible security rules structure is combined with an easy to use GUI.

IMPROVED! Application Activity Control

In this version, application connections are shown better. It allows watching each application in detail by showing addresses, ports and amount of traffic it used. Users can intercept and close any application connection with a simple click.

IMPROVED! Graphical User Interface

The GUI of Comodo Firewall Pro has significant improvements.

- It allows full control over the firewall operations
- It shows a host security index according to the protection level at which it is configured
- Any part of the firewall can be enabled or disabled with one click

IMPROVED! Application Recognition (*Only in Comodo Firewall Pro)*

Comodo Firewall Pro 2 can recognize over 10000 applications and determine their security risks. This database allows users to easily notice if an activity is coming from a safe, virus or spyware program.

Comodo Firewall Pro - Overview

Introduction

Comodo Firewall Pro is designed as an endpoint security enforcer which fulfills all the requirements of a host based security system should do. With its layered security architecture, it is one of the most challenging personal firewalls available, providing an all-in-one security enforcer for all OSI network communication layers. Comodo Firewall Pro includes an ***integrated executable file database***, which is a comprehensive classification of all known executable files. It is the ***only*** firewall which provides such significant information with users.

Network Protection

Comodo Firewall Pro, although designed for personal use, includes an industrial strength stateful inspection firewall, acting at OSI Layers 2, 3 and 4 to filter incoming and outgoing network traffic. Such an advanced filter keeps track of each and every packet sent/received and performs intelligent analysis on critical protocols such as TCP, UDP, FTP etc.
Comodo Firewall Pro also detects and prevents DOS/DDOS attacks including:

- SYN/UDP/ICMP Floods,
- TCP/UDP Port Scans,

Upon facing such an intrusive attack, it switches to an emergency mode by creating some automatic rules and updating its internal states according to the attack behavior, to secure the host against it until the attack ceases. Users will not notice such a change in terms of functionality but will remain protected.

Quick Features:

- Advanced TCP/UDP/ICMP and IP protocol filtering
- IP fragmentation handling
- DOS/DDOS resistance and handling
- Stateful TCP/UDP Protocol Inspection

Application Protection

Although the network protection is adequate to defeat the most of the network based attacks, today's threats require highly sophisticated application based access filtering mechanisms to enforce true host based security policies.
Comodo Firewall Pro provides a powerful application firewall which is one of the best application filters available in the market.
Restricting network traffic according to the application which generates it, requires filtering at OSI Layers 3, 4, 5, 6 and 7.

Application Filtering

Comodo Firewall Pro provides full control on applications' networking behaviors.
Application firewall can:

- Limit applications network access characteristics such as port, protocol and host.
- Give users the ability to control number of connections per minute an application can create.

Leak Resistance

Unfortunately, malware programs are evolving rapidly. Many of such programs employ very advanced techniques to conceal their malicious activities so that they easily bypass the standard protection mechanism provided by the most personal firewalls. These techniques are commonly known as "leak" techniques.

Comodo Firewall Pro passed ALL LEAK TESTS with an outstanding success rate not seen in any other firewalls available.

Although passing the known leak tests are often enough to provide you a robust protection, Trojans do not have to limit themselves to these known techniques and they always try to find new ones to cheat the protection mechanism you have. Due to this fact, Comodo developers constantly research to improve our firewall to keep you protected at all times against emerging and unknown threats.

User Friendliness

Comodo Firewall Pro has an easy to use and intuitive GUI which is suitable for both advanced and novice users.
Our selection of *wizards* make sure novice users will face no difficulties in managing vital security configurations. Advanced users and experts can fine tune Comodo Firewall Pro using its extensive configuration options.

System Requirements

To ensure optimal performance of Comodo Firewall Pro, please ensure that your PC complies with the minimum system requirements as stated below:

- Windows 2000
- Windows XP (All 32 bit versions)
- Internet Explorer Version 5.1 or above
- 64 MB available RAM
- 32 MB of available free hard disk space

Comodo Firewall Installation

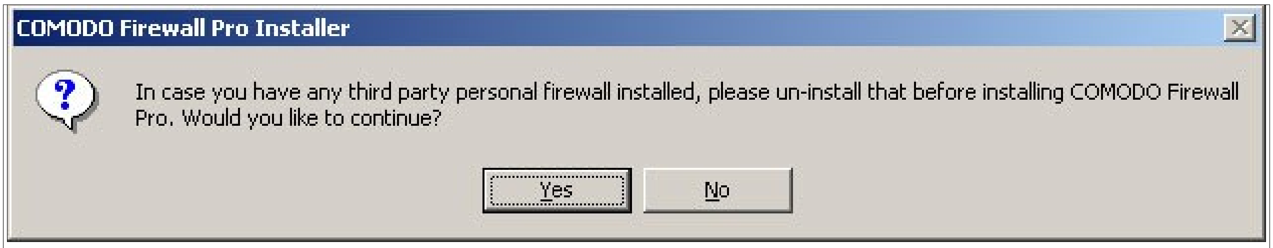
Before you install Comodo Firewall Pro, read the installation instructions carefully and also review the system requirements listed in this chapter.

Installation Process

To install, download the Comodo Firewall Pro setup files to your local hard drive. Next, double click on *downloaded setup* to start the installation wizard and follow the process as below.

STEP 1: Uninstall Other Firewall Programs

1. Before you install Comodo Firewall Pro, you must uninstall any third party Firewall programs installed in your PC. This is necessary as other firewall programs may interfere with the installation of Comodo Firewall Pro and reduce the protection offered by it. Click ***Yes*** to continue.



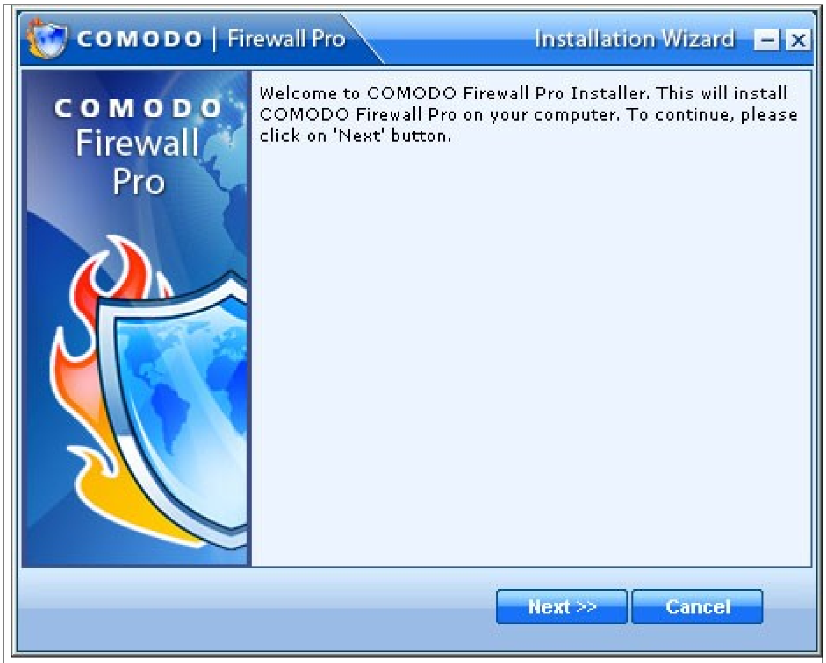
COMODO Firewall Pro Installer

In case you have any third party personal firewall installed, please un-install that before installing COMODO Firewall Pro. Would you like to continue?

Figure: Uninstall Third Party Firewalls

STEP 2 : Welcome Dialogue box

2. The set up program starts automatically and the Welcome wizard is displayed. At this time, you may cancel the install process or continue with the Comodo Firewall Pro Setup program. It is recommended that you exit all Windows programs before running the setup. Click '**Next'** to continue.

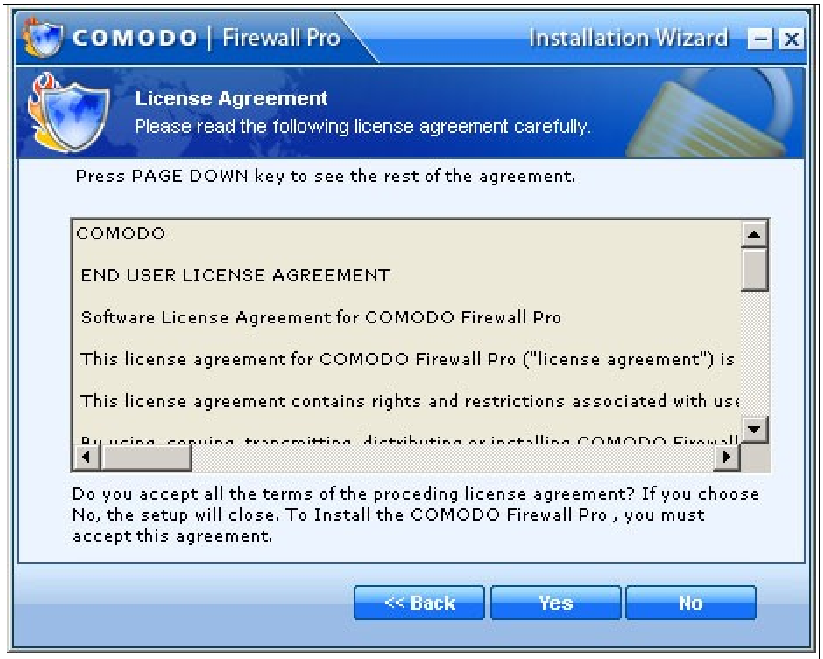


Welcome to COMODO Firewall Pro Installer. This will install COMODO Firewall Pro on your computer. To continue, please click on 'Next' button.

Figure: InstallShield Welcome Wizard

STEP 3: License Agreement

3. When Comodo Firewall Pro is installed for the first time, you must complete the initialization phase by reading and accepting the license agreement. After you read the End-User License Agreement, click **Yes** to continue installation. If you decline, you cannot continue with the installation.



License Agreement

Please read the following license agreement carefully.

Press PAGE DOWN key to see the rest of the agreement.

COMODO

END USER LICENSE AGREEMENT

Software License Agreement for COMODO Firewall Pro

This license agreement for COMODO Firewall Pro ("license agreement") is

This license agreement contains rights and restrictions associated with us

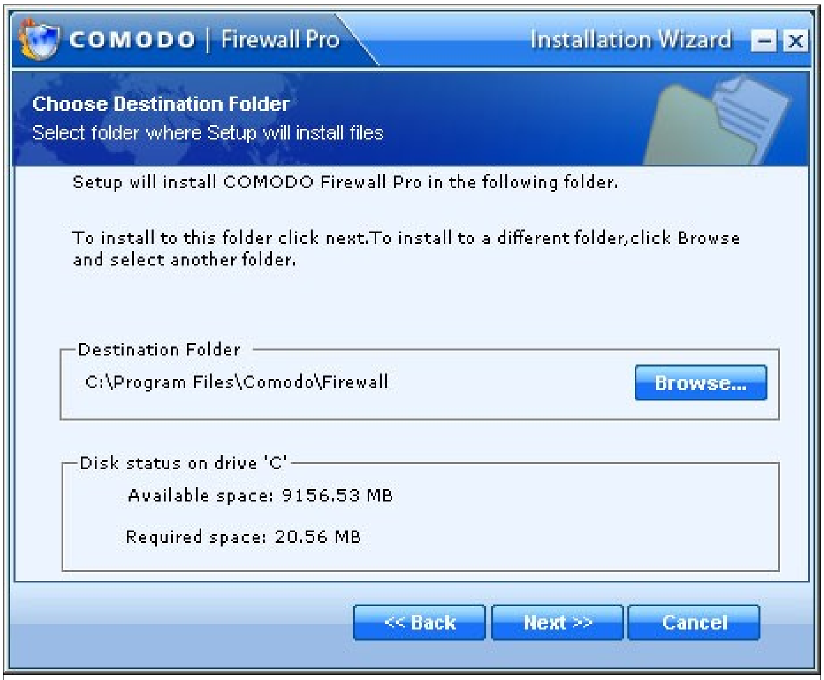
By using, copying, transmitting, distributing or installing COMODO Firewall

Do you accept all the terms of the proceding license agreement? If you choose No, the setup will close. To Install the COMODO Firewall Pro , you must accept this agreement.

Figure: End User License Agreement

STEP 4: Location Destination Folder

4. On the Destination Wizard page, confirm the location of the Firewall installation files. To install the program in the default destination location, click '***Next'***. The default destination directory is the C:\Program Files\Comodo\Firewall.



Choose Destination Folder
Select folder where Setup will install files

Setup will install COMODO Firewall Pro in the following folder.

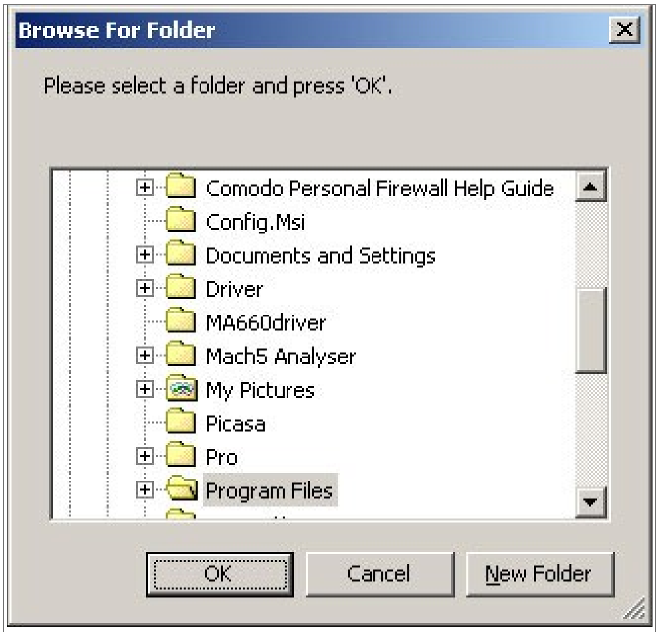
To install to this folder click next.To install to a different folder,click Browse and select another folder.

Destination Folder
C:\Program Files\Comodo\Firewall

Disk status on drive 'C'
Available space: 9156.53 MB
Required space: 20.56 MB

Figure: Default Destination Folder

If you do not wish to install the Firewall files in the default location, to install to a different folder, click ***BROWSE*** and select another folder. Click ***OK*** to continue with the installation process.



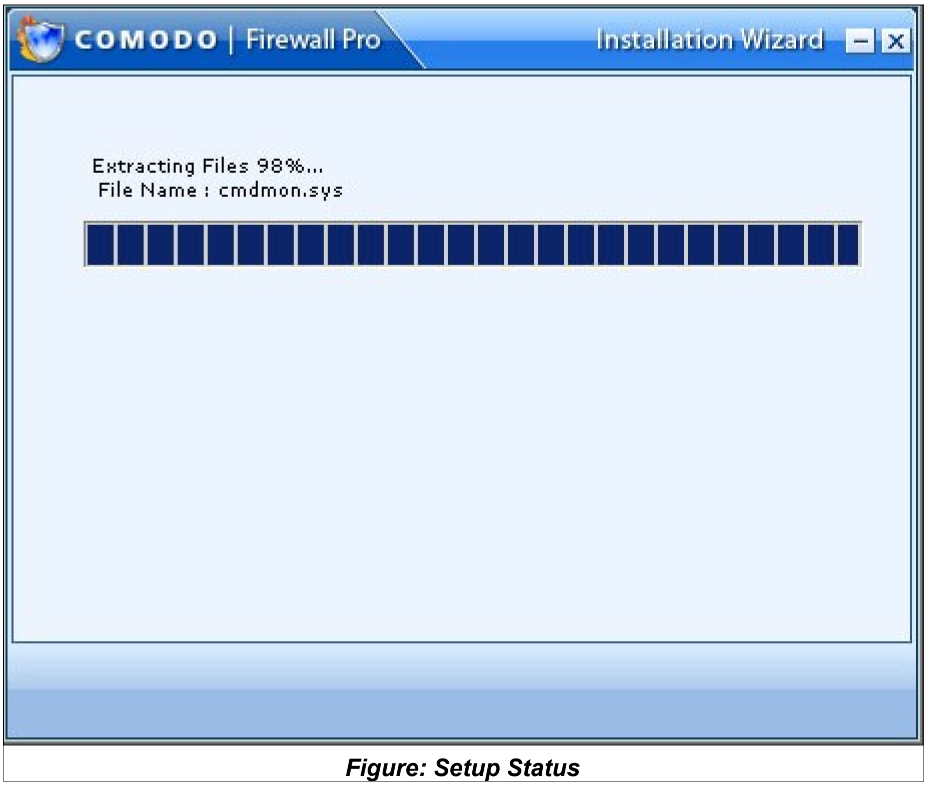
Browse For Folder

Please select a folder and press 'OK'.

Figure: Choose Destination Folder

STEP 5: Set Up Status Box

5. A setup status dialogue box is displayed. You will see a progress bar indicating that files are being installed.

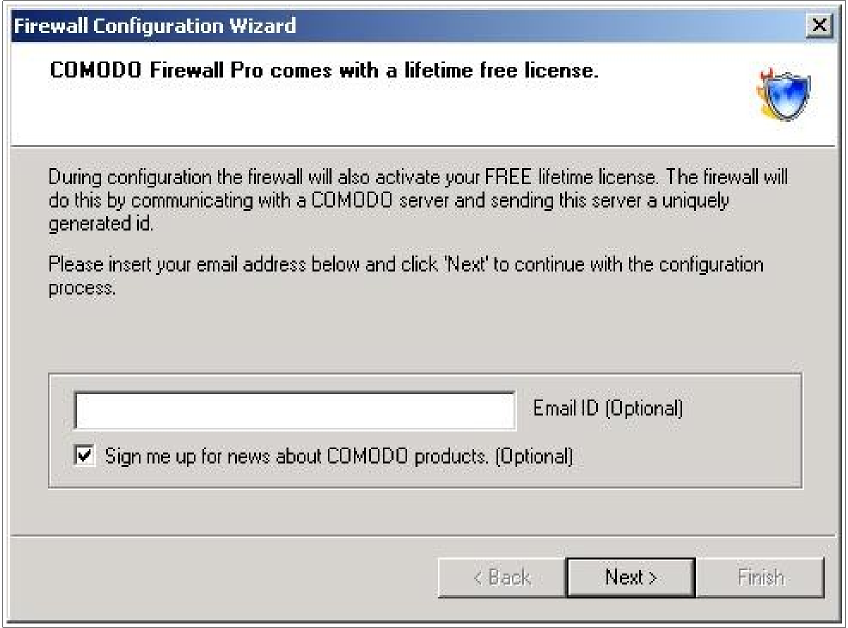


Extracting Files 98%...
File Name : cmdmon.sys

Figure: Setup Status

STEP 6: License Configuration

6. This screen appears only when license is not already activated. Now COMODO Firewall Pro comes with lifetime license on installation itself and so you do not have to activate it again. It does implicit activation and in that process generates a unique id that it sends to a COMODO server. If you wish to sign up for news letter and want to give your e-mail id, you can enter that here. To receive news about Comodo products check the box stating "Sign me up for news about COMODO products", if you don't wish to receive any news from COMODO uncheck the box.



COMODO Firewall Pro comes with a lifetime free license.

During configuration the firewall will also activate your FREE lifetime license. The firewall will do this by communicating with a COMODO server and sending this server a uniquely generated id.

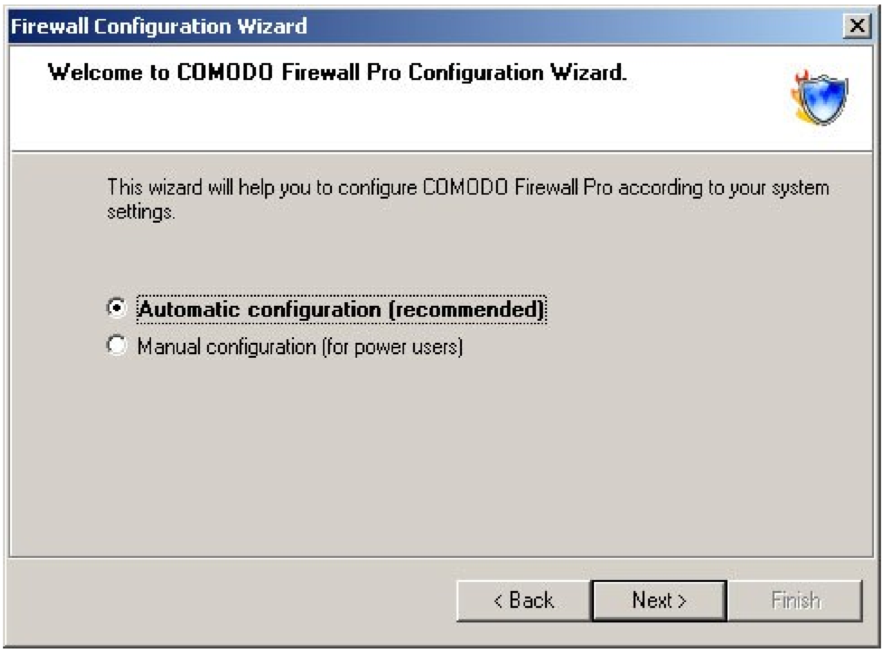
Please insert your email address below and click 'Next' to continue with the configuration process.

Email ID (Optional)

☑ Sign me up for news about COMODO products. (Optional)

STEP 7: Configuration

7. Next, you are presented with a choice of automatic or manually configuration. Automatic configuration is recommended for most users. Manual configuration runs the Add Trusted Zone wizard, the Scan For Known Applications wizard and some basic options outlined in Advanced Configuration.



Firewall Configuration Wizard

Welcome to COMODO Firewall Pro Configuration Wizard.

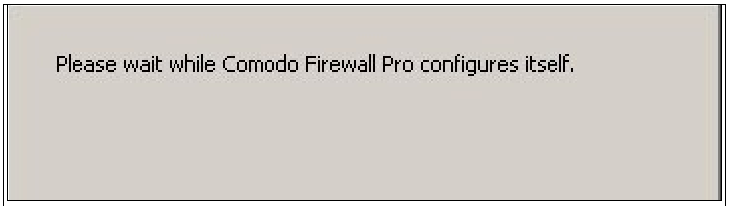
This wizard will help you to configure COMODO Firewall Pro according to your system settings.

● Automatic configuration (recommended)

○ Manual configuration (for power users)

STEP 8: Finalising Installation

8. To complete the installation process, your system will be configured and you will a dialogue box like the one below.

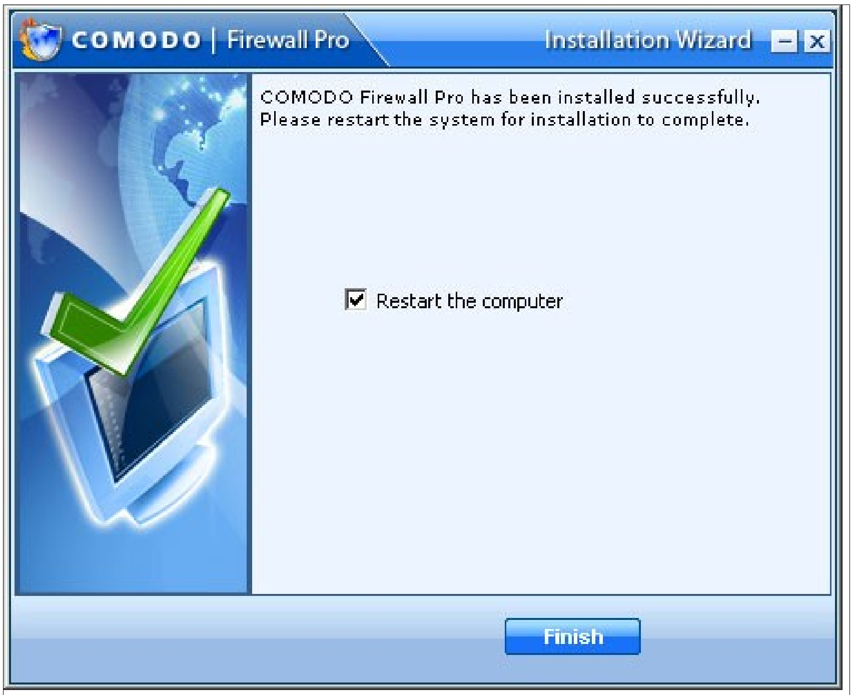


Please wait while Comodo Firewall Pro configures itself.

Figure: Configuring your system

STEP 9: Restart your system

9. A Setup Complete confirmation dialogue box will be displayed indicating successful completion and telling you that you should restart your system now. Please save any unsaved data and click '***Finish'***.



COMODO Firewall Pro has been installed successfully.
Please restart the system for installation to complete.

☑ Restart the computer

Figure: Restart your System

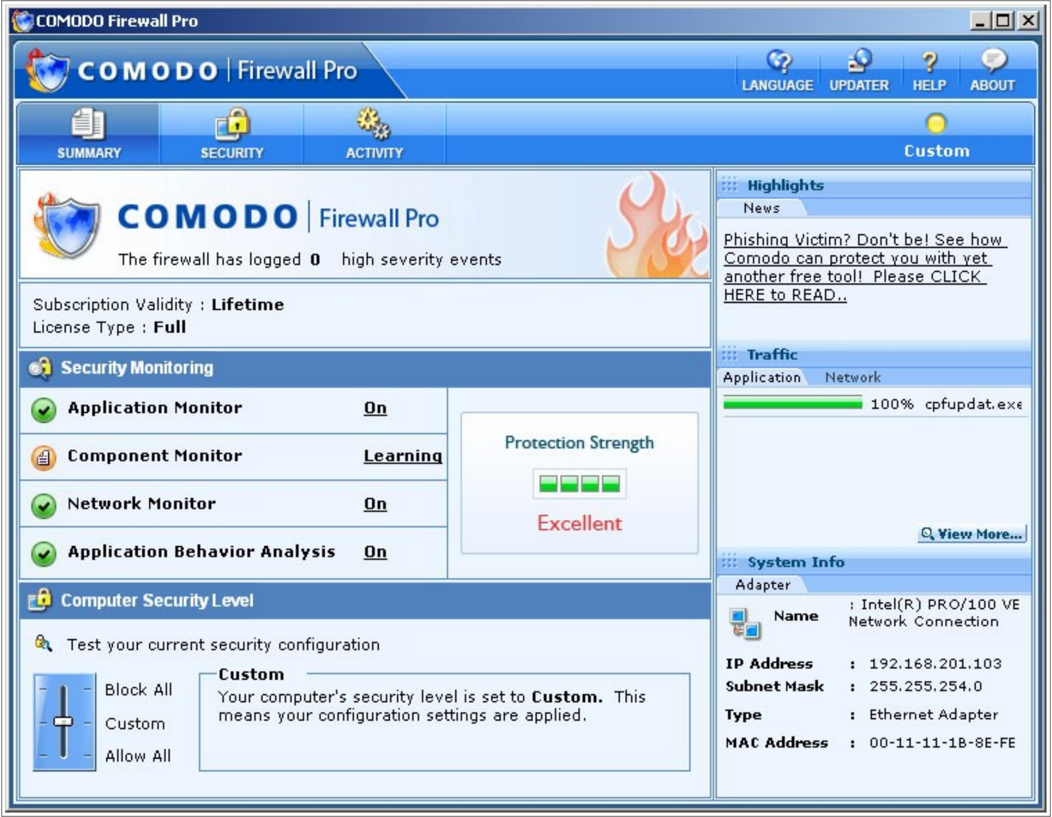
Comodo Firewall Pro Management Interface

After installation, the Comodo Firewall Pro icon will be displayed on the Windows desktop. To start the Comodo Firewall Pro program, double-click on the icon and the management interface will open.

Figure: Comodo Firewall Pro Desktop Shortcut

Your computer is automatically protected by the firewall every time you start it. You do not have to explicitly start the firewall to protect your computer. The start screen of the firewall appears every time you re-start your computer.

Furthermore, the main window of the Comodo Firewall Pro will be opened by default when you re-start your computer. If you choose not to show the application window upon system start-up by unchecking this setting inProgram Settings under Advanced Configuration. Via the main window, the Comodo Firewall Pro is administered. You find information on the main window and on administering the Comodo Firewall Pro in Firewall Summary, Firewall Activity and Firewall Security.



COMODO Firewall Pro

The firewall has logged 0 high severity events

Subscription Validity : **Lifetime**
License Type : **Full**

Highlights
News

Phishing Victim? Don't be! See how Comodo can protect you with yet another free tool! Please CLICK HERE to READ..

Security Monitoring

Application Monitor	On
Component Monitor	Learning
Network Monitor	On
Application Behavior Analysis	On

Protection Strength
🟩🟩🟩🟩
Excellent

Traffic
Application Network
100% cpfupdat.exe
View More...

Computer Security Level

Test your current security configuration

Block All
Custom
Allow All

Custom
Your computer's security level is set to **Custom.** This means your configuration settings are applied.

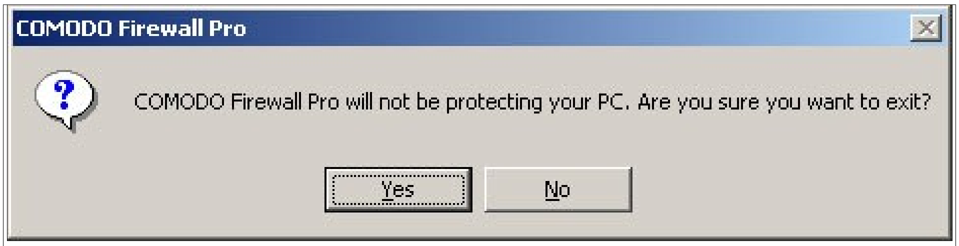
System Info
Adapter

Name	:	Intel(R) PRO/100 VE Network Connection
IP Address	:	192.168.201.103
Subnet Mask	:	255.255.254.0
Type	:	Ethernet Adapter
MAC Address	:	00-11-11-1B-8E-FE

Figure: Comodo Firewall GUI

Closing this window will exit the Comodo Firewall Pro management interface. The firewall will remain active, protecting your computer, in the background.

To completely shut the program down, right-click on the Comodo Firewall Pro and select 'Exit'. If you choose to exit, you will see a dialogue box confirming whether you want to exit or not.



COMODO Firewall Pro

COMODO Firewall Pro will not be protecting your PC. Are you sure you want to exit?

Figure: Exit Comodo Firewall

If you choose to exit, the Firewall will be disabled and will not protect your PC.

Comodo Firewall Pro Multi-Language Installation

You can choose to use Comodo Firewall Pro in any one of 13 languages. English language support is also included with each of the multi-language versions.

You have two main installation options

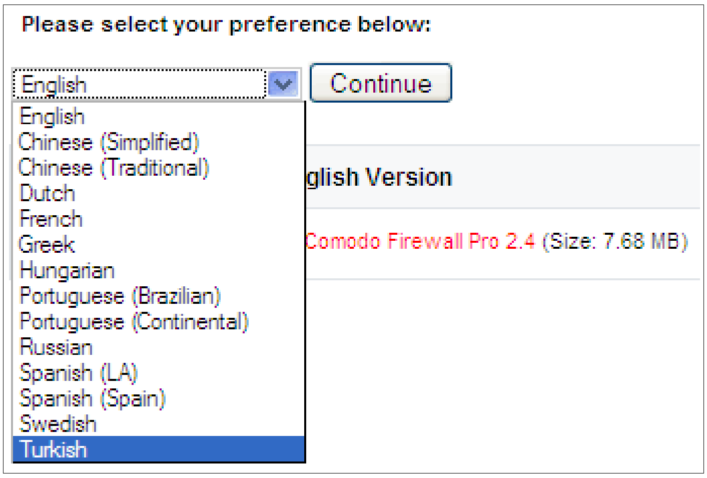
1. Installing a foreign language version of the application

[2. Adding foreign language support to an existing installation (version 2.4 and above only)]

Installing a foreign language version of the application

You should pick this option if you do NOT have Comodo Firewall Pro 2.4 or above installed or have an earlier version installed that you need to update. Using this option will download and install the latest version of the firewall in the language you choose.

Please visit http://www.personalfirewall.comodo.com/download_firewall.html to make your choice of language.

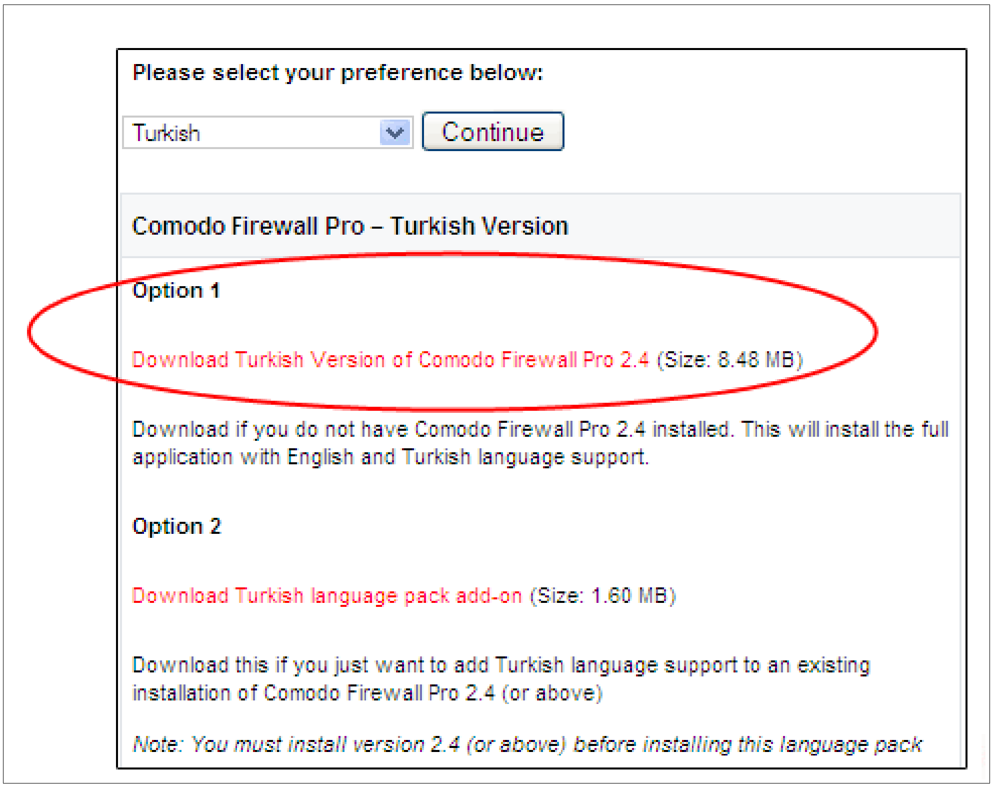


Please select your preference below:

glish Version

Comodo Firewall Pro 2.4 (Size: 7.68 MB)

You will then be presented with two download Options. You should choose Option 1 because this is a clean install of the firewall in your choice of language.



Please select your preference below:

Comodo Firewall Pro – Turkish Version

Option 1

Download Turkish Version of Comodo Firewall Pro 2.4 (Size: 8.48 MB)

Download if you do not have Comodo Firewall Pro 2.4 installed. This will install the full application with English and Turkish language support.

Option 2

Download Turkish language pack add-on (Size: 1.60 MB)

Download this if you just want to add Turkish language support to an existing installation of Comodo Firewall Pro 2.4 (or above)

Note: You must install version 2.4 (or above) before installing this language pack

You will now be taken through the firewall installation and setup process as outlined in Comodo Firewall Pro Installation.

After setup, you can switch between languages at any time by click the 'Language' button.

Adding a language pack to an existing installation:

If you already installed Comodo Firewall Pro 2.4 or above then you can ADD support for a specific language.

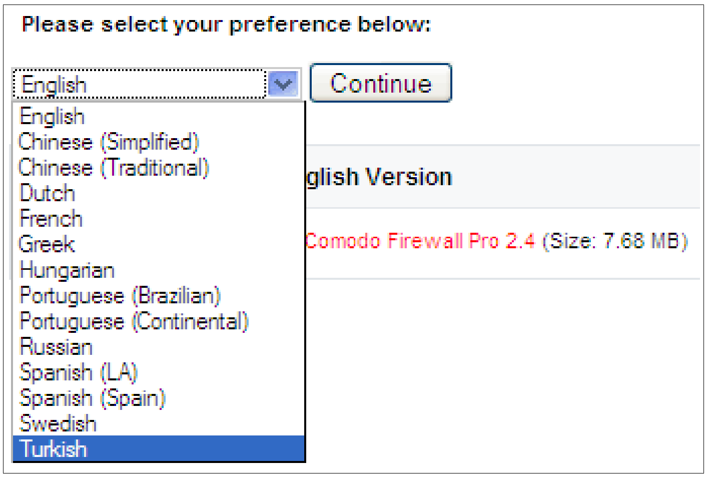
Installing an additional language pack to Comodo Firewall Pro English Version

To install a language pack, follow the steps below.

STEP 1: Download your language pack at the Comodo Website

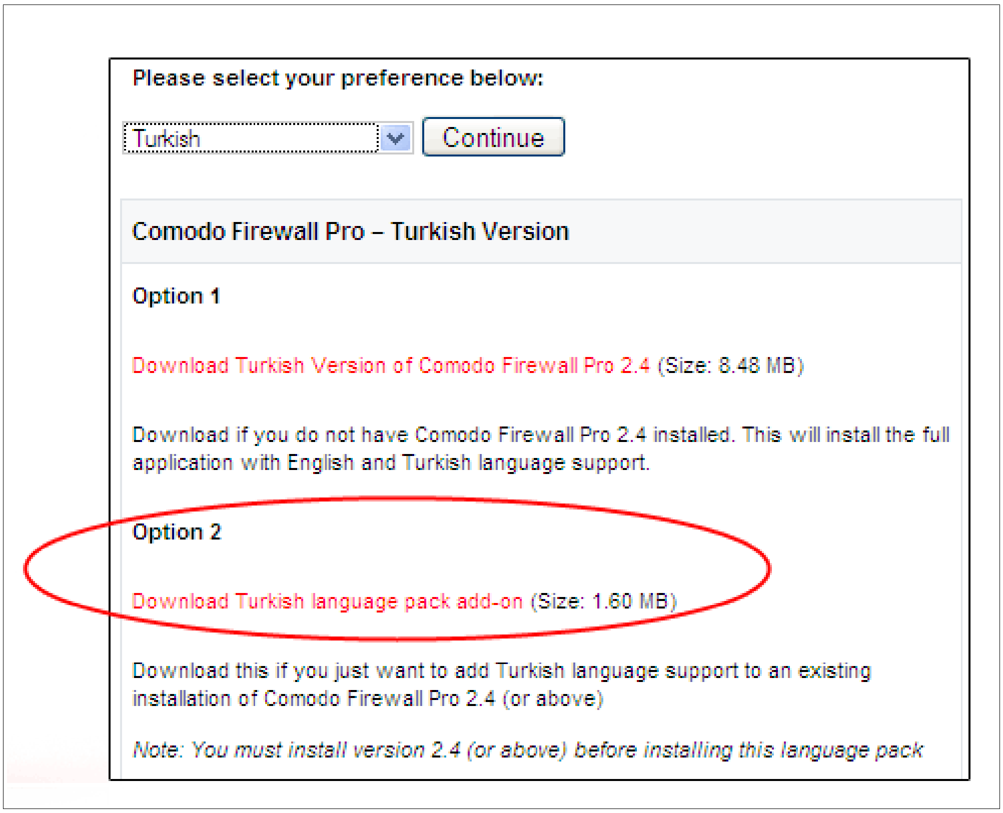
1. Assuming you have installed firewall 2.4 or above, please visit http://www.personalfirewall.comodo.com/download_firewall.html to begin the language selection process.

Choose your preferred language from the drop down box. In the example below, we have chosen to install Turkish as an additional language.


Please select your preference below:

Click 'Continue'.

You will then be presented with two download Options. You should choose Option 2 because you are adding Turkish language support to an existing installation of the firewall.



Please select your preference below:

Turkish

Comodo Firewall Pro – Turkish Version

Option 1

Download Turkish Version of Comodo Firewall Pro 2.4 (Size: 8.48 MB)

Download if you do not have Comodo Firewall Pro 2.4 installed. This will install the full application with English and Turkish language support.

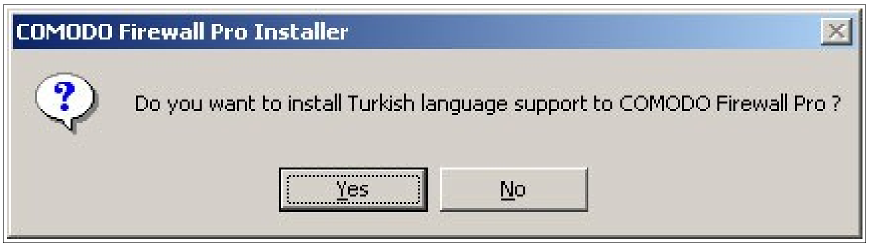
Option 2

Download Turkish language pack add-on (Size: 1.60 MB)

Download this if you just want to add Turkish language support to an existing installation of Comodo Firewall Pro 2.4 (or above)

Note: You must install version 2.4 (or above) before installing this language pack

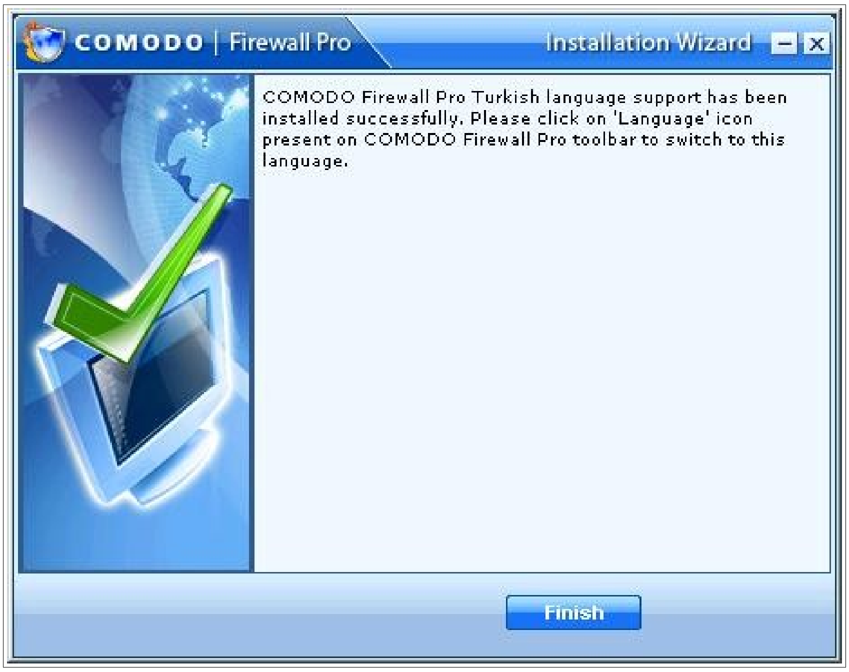
Click ***Yes*** at the confirmation box to start the installation of your additional language.



COMODO Firewall Pro Installer

Do you want to install Turkish language support to COMODO Firewall Pro ?

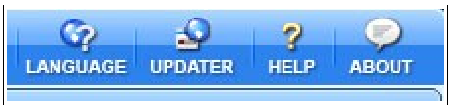
After installing the additional language you will see the following confirmation screen.Click Finish to complete the installation.



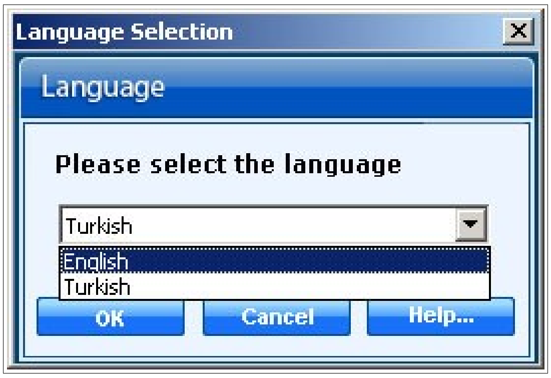
COMODO Firewall Pro Turkish language support has been installed successfully. Please click on 'Language' icon present on COMODO Firewall Pro toolbar to switch to this language.

STEP 2: Switching between languages in Comodo Firewall Pro

To switch between languages, first select the 'LANGUAGE' button at the top right of the firewall interface (shown below)



Select the language you wish to select from the list of languages displayed in the Language Selection. Click OK to proceed.

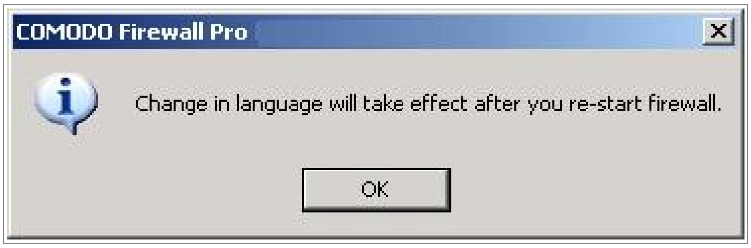


Please select the language

Turkish

English
Turkish

Select 'OK' to confirm your choice.



COMODO Firewall Pro

Change in language will take effect after you re-start firewall.

In order for your choice to take effect, you must restart the firewall. You can do this by either:

(i) Restarting your computer (recommended)

(ii) Closing then restarting the firewall by right clicking on the firewall tray icon and selecting 'Exit'. To restart the firewall, select Start>Comodo>Firewall>Comodo Firewall Pro.

The firewall will be in your choice of language the next time you restart the application.

Comodo Firewall Uninstallation

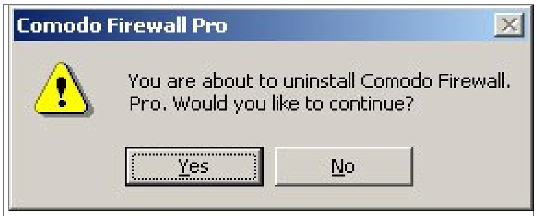
If you need to uninstall Comodo Firewall Pro, do the following:

1. Click the Windows Start button and browse to All Programs>Comodo>Firewall>Uninstall

OR

- On the Windows taskbar, click Start > Settings > Control Panel.
- In the Control Panel, double-click Add/Remove Programs.
- In the list of currently installed programs, click Comodo Firewall Pro.
- Click Change/Remove.

2. A dialogue box appears asking for confirmation of uninstallation. Click ***Yes*** to uninstall.

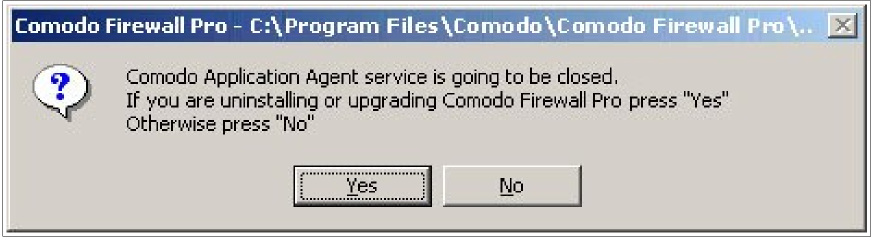


Comodo Firewall Pro

You are about to uninstall Comodo Firewall. Pro. Would you like to continue?

Figure: Uninstall CPF configuration settings

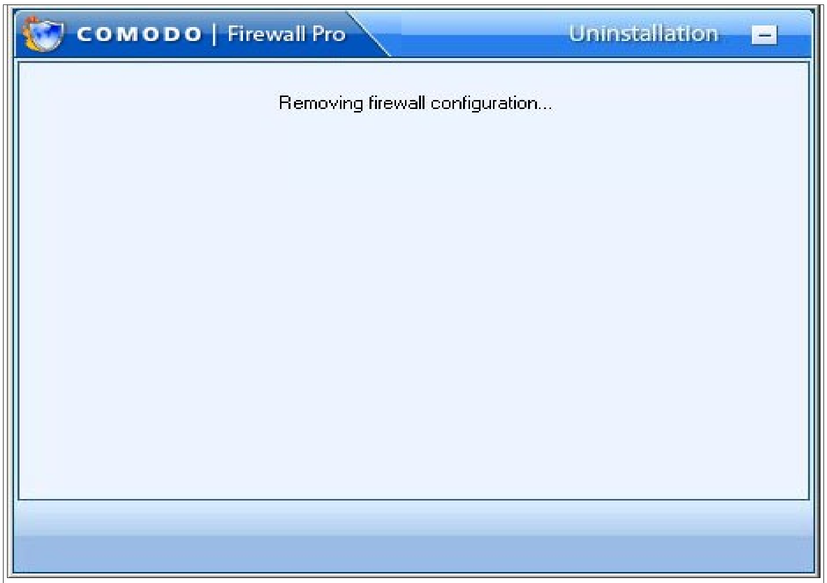
3. Next, the firewall notifies you that the Comodo Application Agent is to be shut down. Click ***Yes*** to continue uninstallation



Comodo Firewall Pro - C:\Program Files\Comodo\Comodo Firewall Pro\..

Comodo Application Agent service is going to be closed.
If you are uninstalling or upgrading Comodo Firewall Pro press "Yes"
Otherwise press "No"

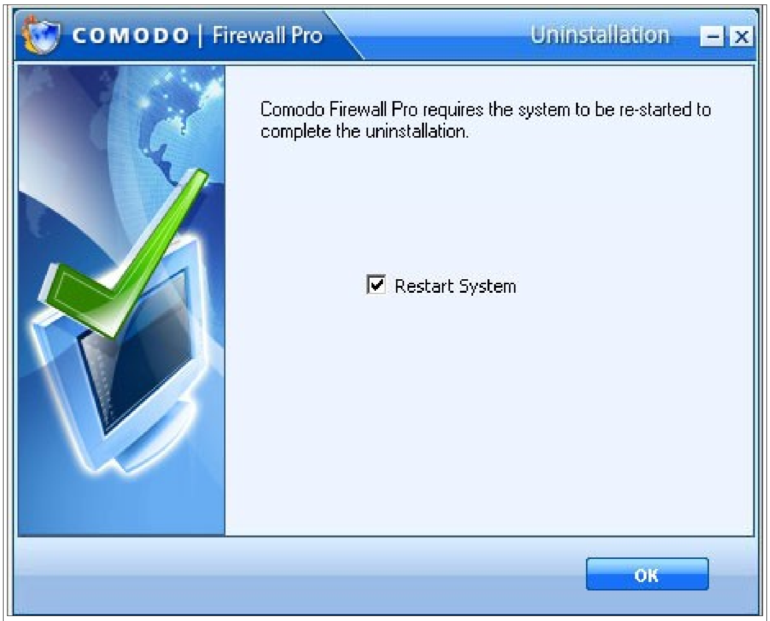
4. A Setup Status dialogue box informs you that un-installation is taking place.



Removing firewall configuration...

Figure: Uninstall CPF

5. After un-installation, InstallShield Wizard appears. Check the Restart Computer box and click 'OK' to complete the un-installation.



Comodo Firewall Pro requires the system to be re-started to complete the uninstallation.

☑ Restart System

Figure: Restart Your Computer

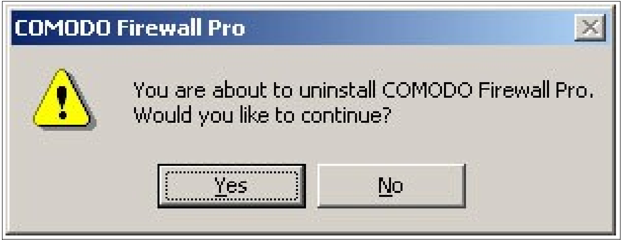
Comodo Firewall Pro Multi-Language Uninstallation

Uninstalling an Addon

You can uninstall Multi-Languages in Comodo Firewall Pro as follows.

STEP 1: Uninstalling Comodo Firewall Pro

1. To uninstall an addon, Click Start>Programs>Comodo>Firewall>Uninstall, you would get the following screen.To proceed with uninstallion Click Yes to continue.

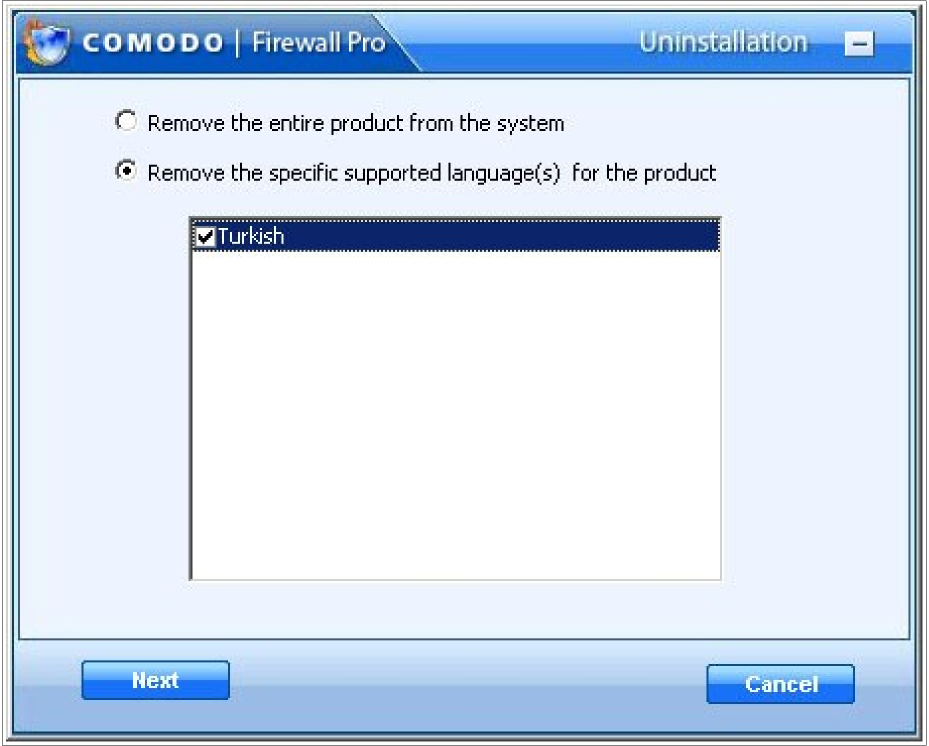


COMODO Firewall Pro

You are about to uninstall COMODO Firewall Pro.
Would you like to continue?

STEP 2: Uninstalling a Specific Language

2. To uninstall Comodo Firewall Pro from the system select "Remove the entire product from the system". To remove a specific language select "Remove the specific supported language(s) for the product" and Select the language which you need uninstall from the list of languages appearing in this section. Then Click Next to proceed or Click Cancel to exit the uninstallion wizard.



COMODO | Firewall Pro Uninstallation

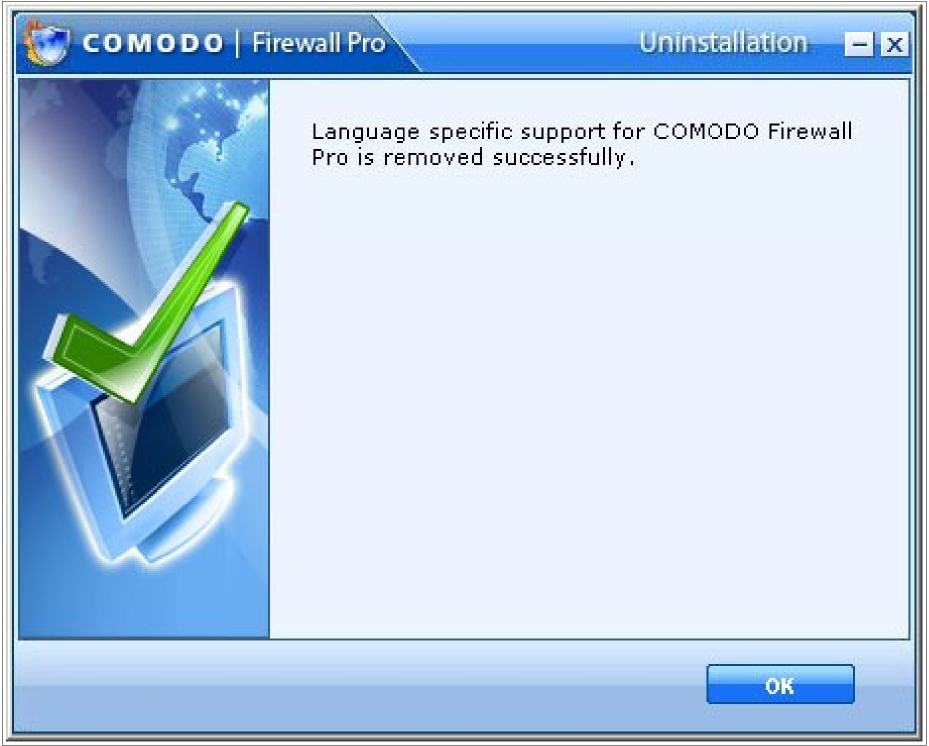
○ Remove the entire product from the system

● Remove the specific supported language(s) for the product

☑ Turkish

STEP 3: Finish

3. Once the uninstallation of the language is finished, the following screen would appear.



Language specific support for COMODO Firewall Pro is removed successfully.

Starting Comodo Firewall

After installation, Comodo Firewall Pro will automatically start whenever you start Windows. In order to configure and view settings within Comodo Firewall Pro you need to access the management interface.

There are 3 different ways to access the management interface of Comodo Firewall Pro - System Tray Icon, via Windows Desktop, via the Windows Start menu.

1. Comodo Firewall Pro Tray Icon

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

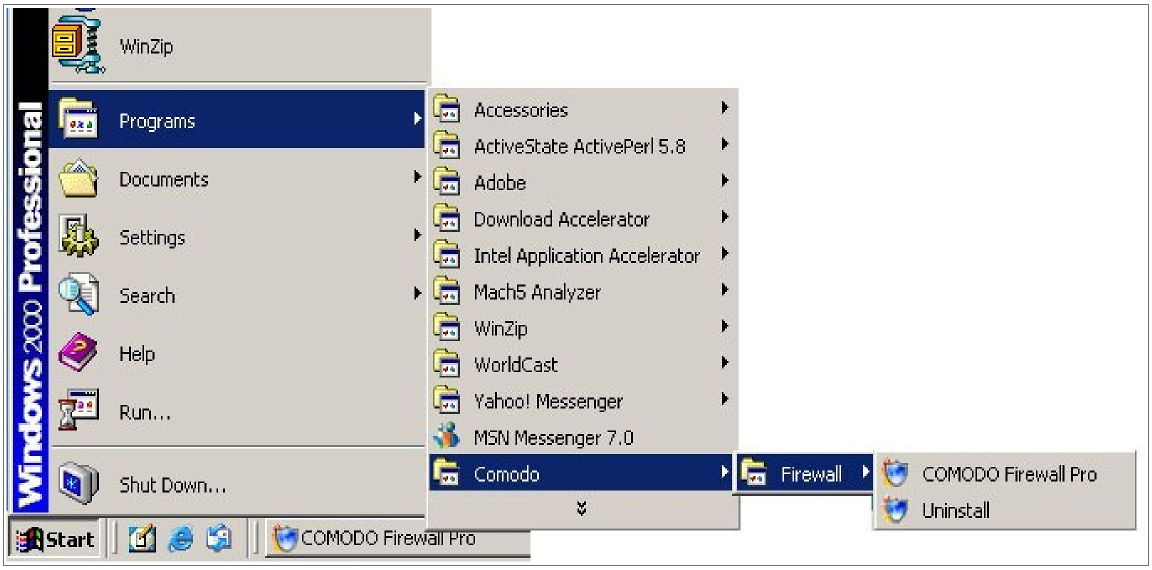
2. Windows Desktop

Just double click the shield icon in the desktop to start Comodo Firewall Pro.

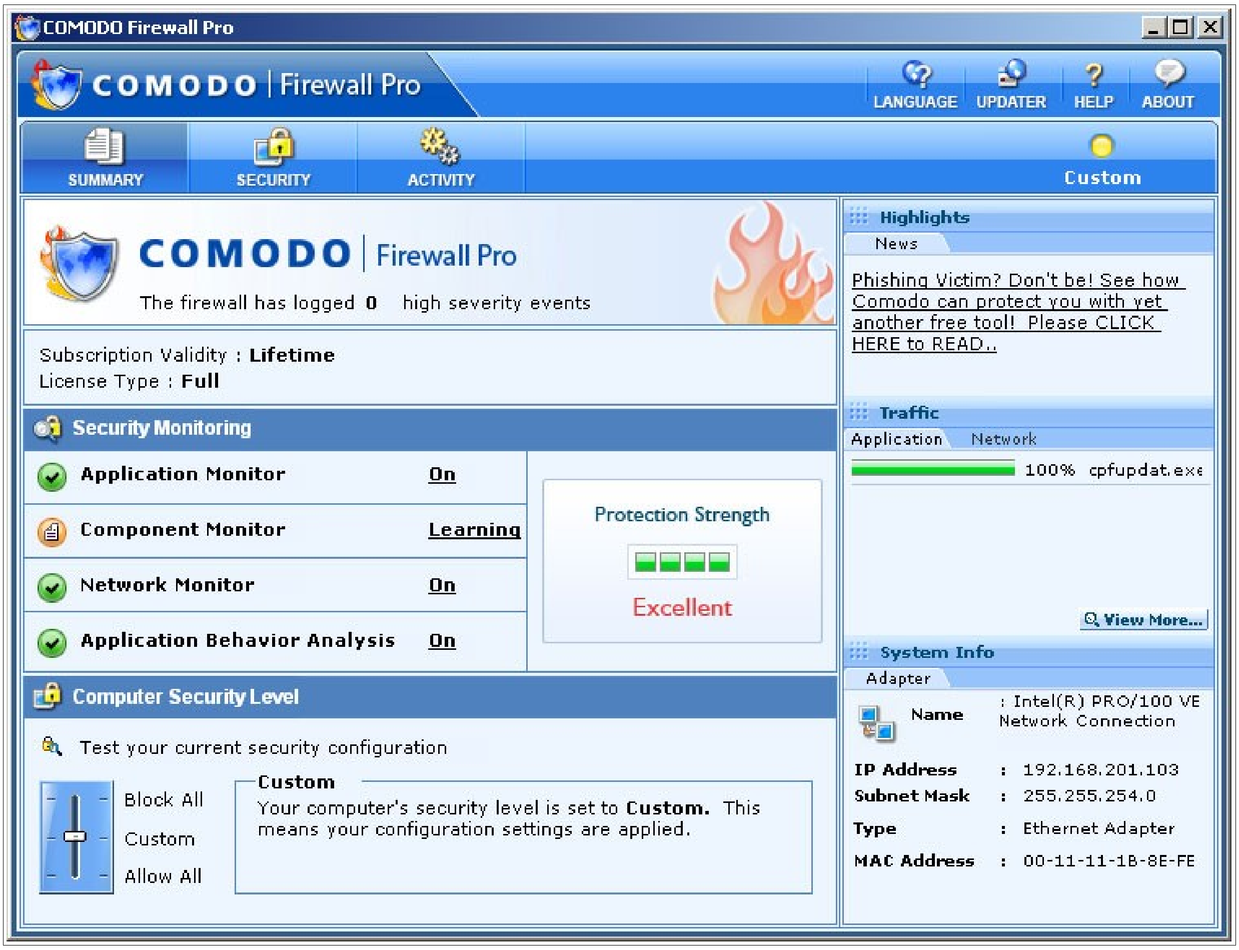
3. Start Menu

You can also access Comodo Firewall via the Windows Start Menu.

Click 'Start' and select Programs->Comodo->Firewall->Comodo Firewall Pro



Using any of the methods outlined above will lead you to the main interface as shown below:



COMODO | Firewall Pro

The firewall has logged 0 high severity events

Subscription Validity : **Lifetime**
License Type : **Full**

Security Monitoring

Application Monitor	On
Component Monitor	Learning
Network Monitor	On
Application Behavior Analysis	On

Protection Strength
Excellent

Computer Security Level

Test your current security configuration

Block All
Custom
Allow All

Custom
Your computer's security level is set to **Custom.** This means your configuration settings are applied.

Highlights
News

Phishing Victim? Don't be! See how Comodo can protect you with yet another free tool! Please CLICK HERE to READ..

Traffic
Application Network

100% cpfupdat.exe

View More...

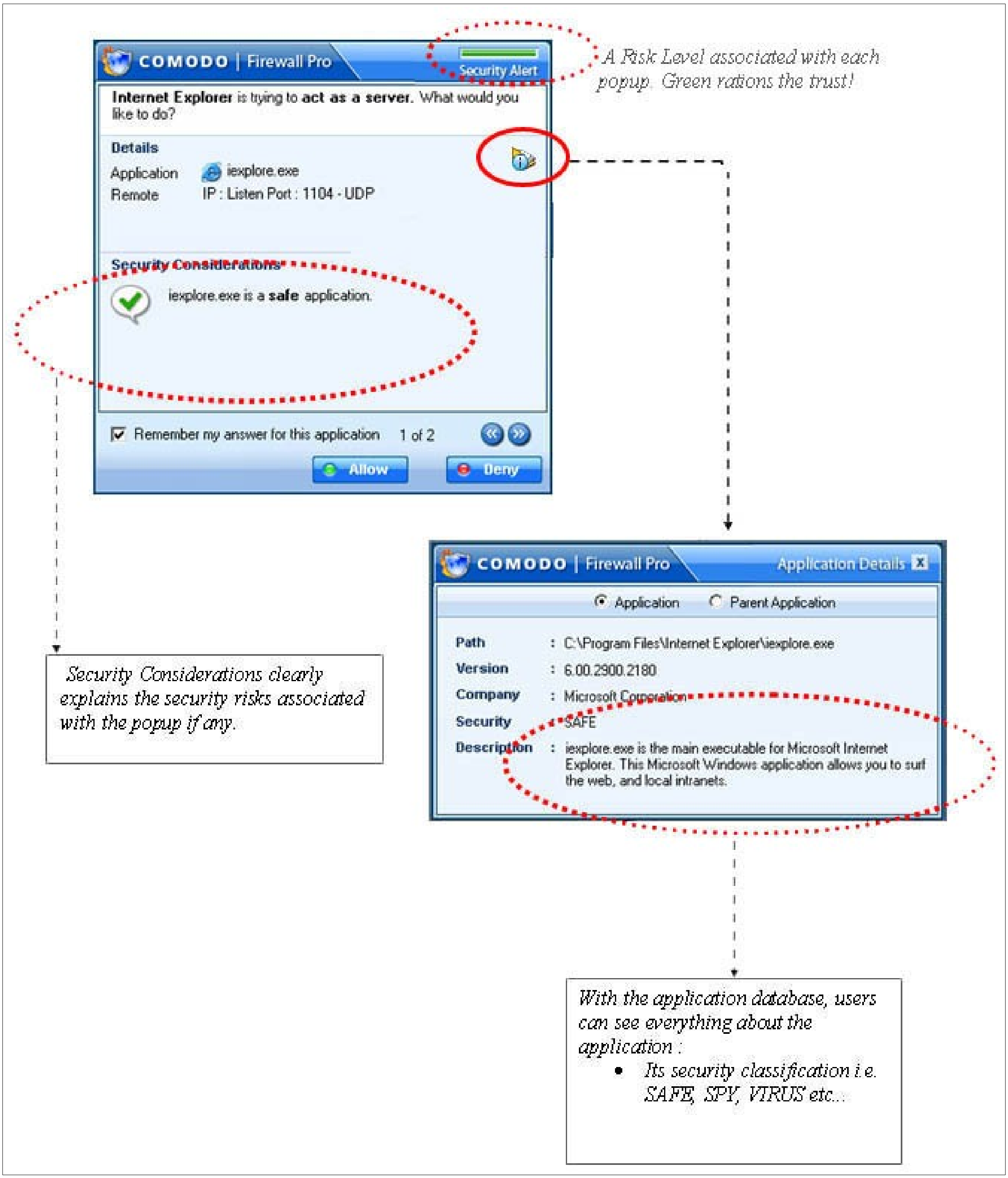
System Info
Adapter

Name	:	Intel(R) PRO/100 VE Network Connection
IP Address	:	192.168.201.103
Subnet Mask	:	255.255.254.0
Type	:	Ethernet Adapter
MAC Address	:	00-11-11-1B-8E-FE

Understanding Alerts

You may see an alert message for example, if an application for which you have not set rules tries to access your network connection. In this case firewall asks you whether to allow or deny access.

The basic layout of a Comodo Firewall Pro Alert is illustrated below:



Internet Explorer is trying to **act as a server**. What would you like to do?

Details

Application iexplore.exe

Remote IP : Listen Port : 1104 - UDP

Security Considerations

iexplore.exe is a **safe** application.

☑ Remember my answer for this application 1 of 2

● Application ○ Parent Application

Path : C:\Program Files\Internet Explorer\iexplore.exe

Version : 6.00.2900.2180

Company : Microsoft Corporation

Security : SAFE

Description : iexplore.exe is the main executable for Microsoft Internet Explorer. This Microsoft Windows application allows you to surf the web, and local intranets.

A Risk Level associated with each popup. Green rations the trust!

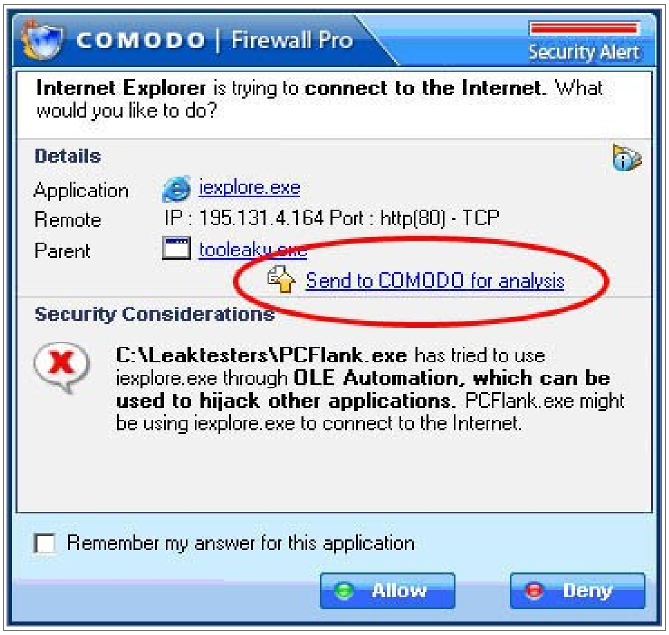
Security Considerations clearly explains the security risks associated with the popup if any.

With the application database, users can see everything about the application :

- *Its security classification i.e. SAFE, SPY, VIRUS etc...*

The Alert includes information like name of **Application** which triggered the alert, the **Parent Application** , the Protocol used by the Application, its IP address and its Port Number.

Some alerts contain the "Send files to COMODO for analysis" link. This happens in cases where Comodo Firewall Pro contains no advice about the application or parent applications and it is notare not in our safe list.



Internet Explorer is trying to **connect to the Internet.** What would you like to do?

Details

Application iexplore.exe
Remote IP : 195.131.4.164 Port : http(80) - TCP
Parent tooleaky.exe
Send to COMODO for analysis

Security Considerations

C:\Leaktesters\PCFlank.exe has tried to use iexplore.exe through **OLE Automation, which can be used to hijack other applications.** PCFlank.exe might be using iexplore.exe to connect to the Internet.

□ Remember my answer for this application

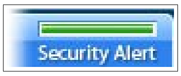
Clicking this link begins the file submission process outlined later in this guide.

What Alerts tell you

Risk Level

The top right corner of the pop up also shows the Security Alert Severity Level. The colour assignations correspond to those outlined in High, Medium and Low Severity Alerts.

For example, the alert shown above indicates a green severity security level:


Security Alert

This is because Internet Explorer is considered a safe application. Quickly glancing at the alert level indicator provides a quick way to determine whether an application or activity should concern the user.

Details

Contains:

- The application name
- The IP address of the site it is attempting to connect to
- The port it is using to make the connection

- The protocol it is using to facilitate the connect

Security Considerations

This area provides a consise, at a glance summary of the security risk involved with allowing this application to access the internet. For a more detailed explanation of the type of information you will see in this area, please refer to Types of Alerts

Choose options

Once you understand the risk, you can respond in the following ways :

Remember my answer for this application: check this box to instruct the Firewall not to generate an alert again if the parameters of the application are the same.

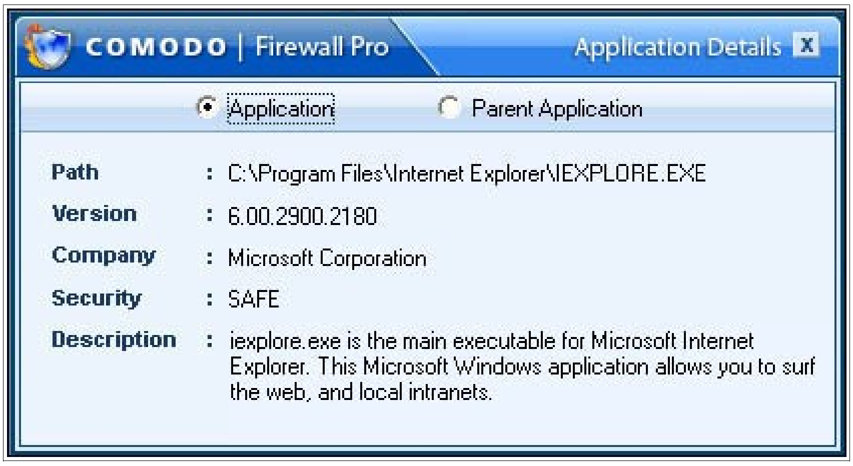
Allow - allows the current instance of the application to access the internet according to the delinated parameters

Deny - Blocks the application from accessing the internet

More Details

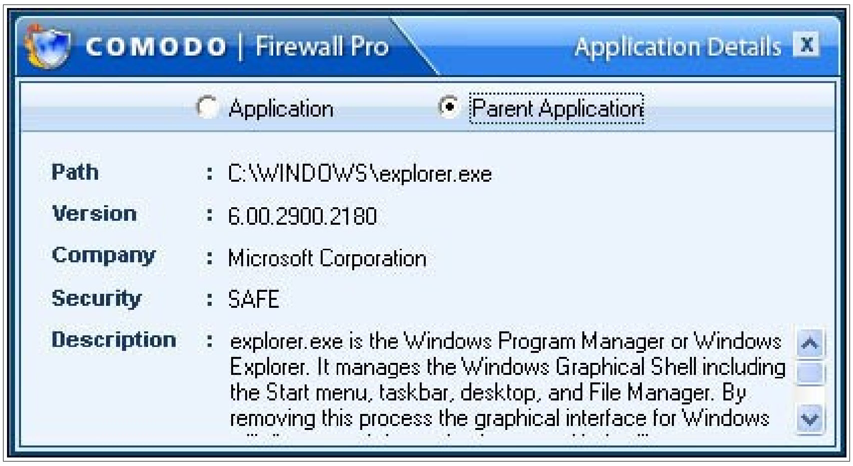
If you are unsure about the application, you can view more information about the application by clicking the more details icon:

When you click More Details, a dialog window will appear with detailed information about the application - helping you decide what to do:



Path : C:\Program Files\Internet Explorer\IEXPLORE.EXE
Version : 6.00.2900.2180
Company : Microsoft Corporation
Security : SAFE
Description : iexplore.exe is the main executable for Microsoft Internet Explorer. This Microsoft Windows application allows you to surf the web, and local intranets.

Selecting the 'Parent Application' radio button enables the user to view information about the application that originally caused the child application to try to access the internet. In this case, Explorer.exe commanded Internet Explorer.exe to access the internet. 'Explorer.exe' is therefore the parent application to 'Internet Explorer.exe'.



○ Application ● Parent Application

Path : C:\WINDOWS\explorer.exe
Version : 6.00.2900.2180
Company : Microsoft Corporation
Security : SAFE
Description : explorer.exe is the Windows Program Manager or Windows Explorer. It manages the Windows Graphical Shell including the Start menu, taskbar, desktop, and File Manager. By removing this process the graphical interface for Windows

Types of Alerts

The 'Security Considerations' section of each pop-up alert contains an icon that provides an at-a-glance information about the type of connection being attempted.

SAFE : you can safely approve this connection request. The 'Remember my answer for this application' option is automatically pre-selected for safe requests.

✓

SUSPICIOUS CONNECTION : Only allow this connection after careful consideration. It might be a leak attack, trojan or spyware risk.

✗

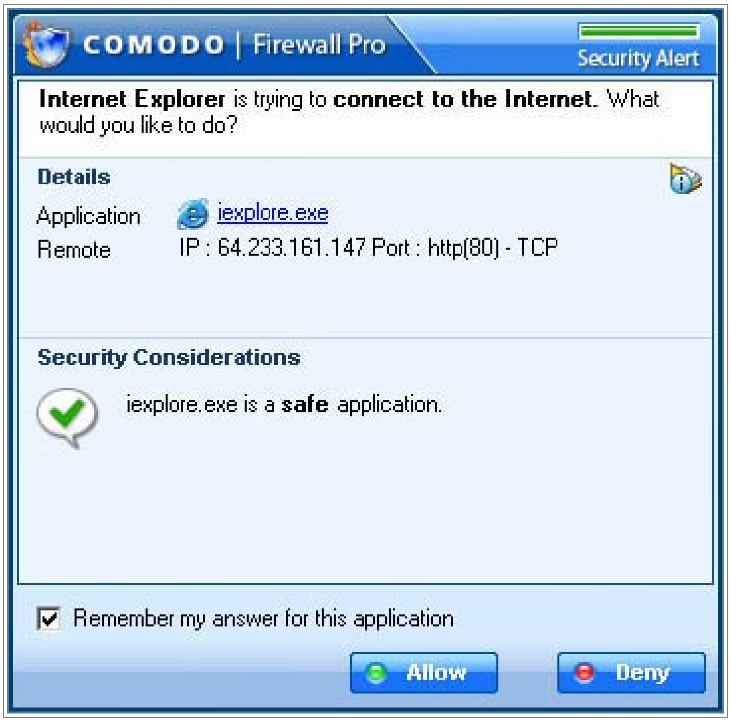
UNKNOWN COMPONENTS DETECTED : Users should click on 'Show Libraries' button and choose what to do with all detected components.

−

UKNOWN REQUEST: Comodo Firewall Pro does not know for sure whether the connection is safe. Proceed with caution.

Common Examples

Incoming Connection Alert : This type of alert is generated when an application is trying to access your computer or network.



Internet Explorer is trying to **connect to the Internet**. What would you like to do?

Details

Application iexplore.exe

Remote IP : 64.233.161.147 Port : http(80) - TCP

Security Considerations

iexplore.exe is a **safe** application.

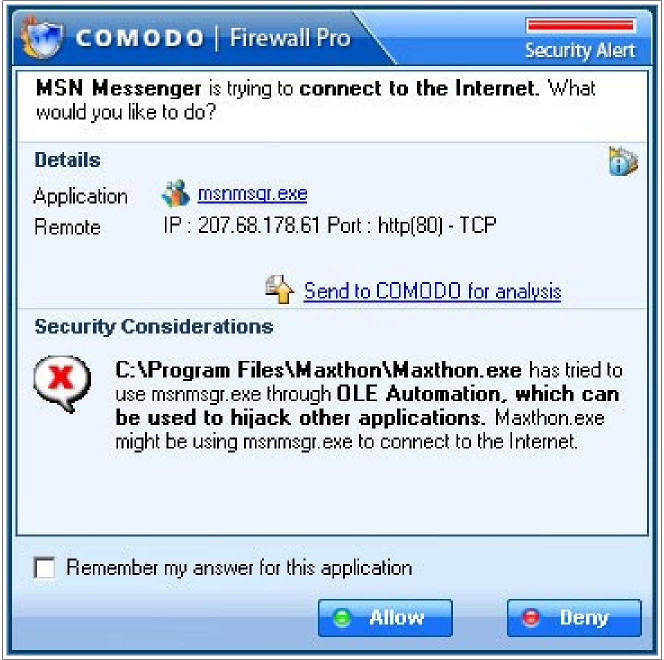
☑ Remember my answer for this application

In case you are unsure about the application , you can view more information about the application by clicking More Info tab so that you can decide on the action to be taken.

When you click the 'More Details' icon , a dialog box will appear containing detailed information about the application.

Outgoing Connection Alert: This type of alert is generated when an application is trying to access your the internet or remote host.

You can choose to allow/deny the application by selecting IP address , Port and Zone in the same way as for Incoming alert. You can also choose whether or not you want the firewall to remember this setting by checking the box at the lower right hand corner.



MSN Messenger is trying to **connect to the Internet**. What would you like to do?

Details

Application msnmsgr.exe

Remote IP : 207.68.178.61 Port : http(80) - TCP

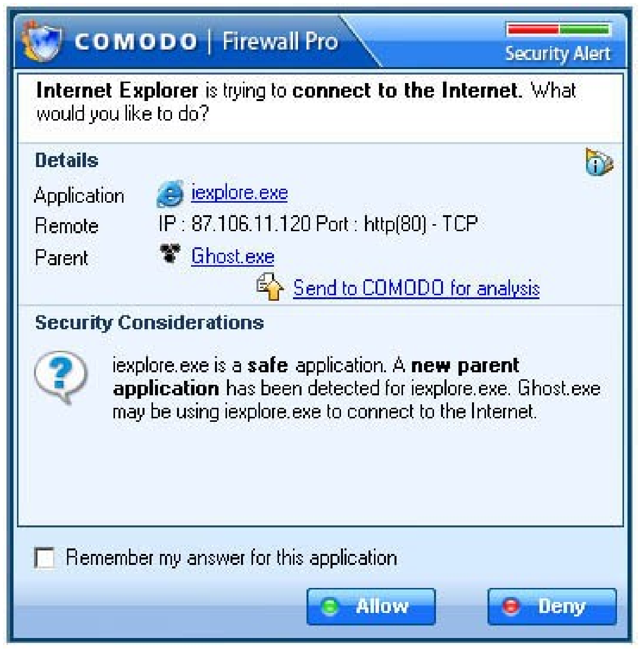
Send to COMODO for analysis

Security Considerations

C:\Program Files\Maxthon\Maxthon.exe has tried to use msnmsgr.exe through **OLE Automation, which can be used to hijack other applications.** Maxthon.exe might be using msnmsgr.exe to connect to the Internet.

☐ Remember my answer for this application

New Parent Application Detected - Parent applications are those that instruct another program to make a connection to the intenet. Often, this is the result of user action and is innocuous. For example, you might click in on link in a email in Microsoft Outlook. Outlook would then tell Internet Explorer to connect to the 'net and would thus become its 'parent' application.



Internet Explorer is trying to **connect to the Internet**. What would you like to do?

Details

Application iexplore.exe
Remote IP : 87.106.11.120 Port : http(80) - TCP
Parent Ghost.exe

Send to COMODO for analysis

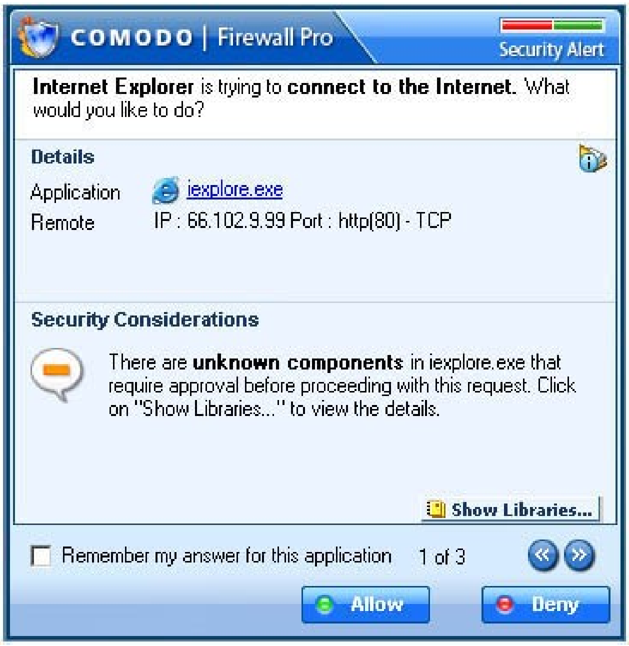
Security Considerations

iexplore.exe is a **safe** application. A **new parent application** has been detected for iexplore.exe. Ghost.exe may be using iexplore.exe to connect to the Internet.

□ Remember my answer for this application

Other times, the connection is not so harmless. In the example below, the malicious program, Ghost.exe has instructed Internet Explorer to connect to the internet. Please monitor every alert you receive to ensure your PC is not subject to outgoing or incoming attacks from hackers, spyware or trojan horse programs.

Unknown Components Detected



Internet Explorer is trying to **connect to the Internet**. What would you like to do?

Details

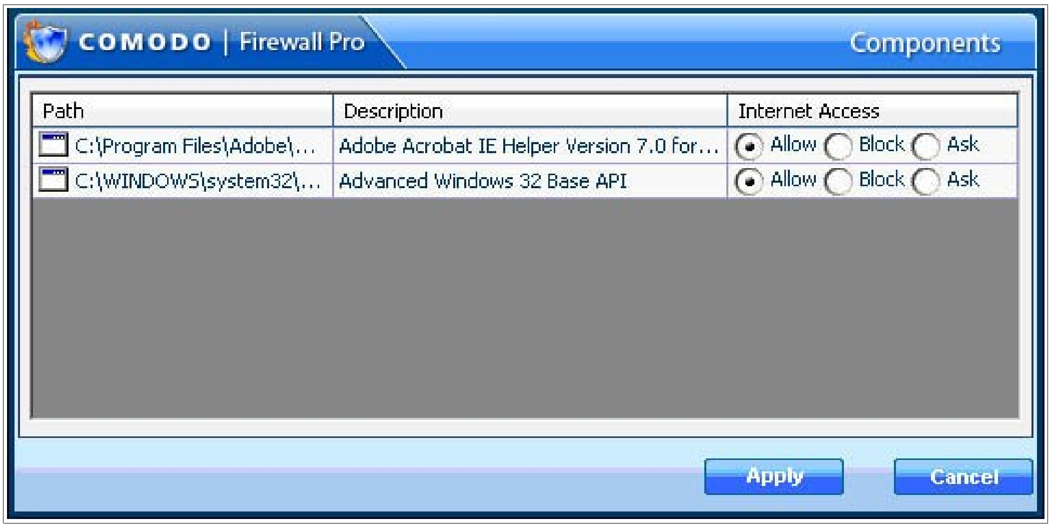
Application iexplore.exe
Remote IP : 66.102.9.99 Port : http(80) - TCP

Security Considerations

There are **unknown components** in iexplore.exe that require approval before proceeding with this request. Click on "Show Libraries..." to view the details.

□ Remember my answer for this application 1 of 3

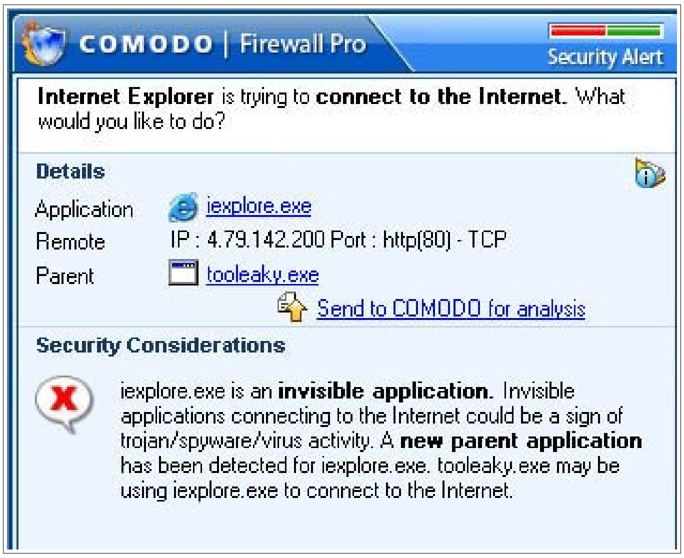
Users should click the 'Show Libraries' button before deciding whether to let the connection proceed:



Path	Description	Internet Access
C:\Program Files\Adobe\...	Adobe Acrobat IE Helper Version 7.0 for...	● Allow ○ Block ○ Ask
C:\WINDOWS\system32\...	Advanced Windows 32 Base API	● Allow ○ Block ○ Ask

Invisible Application : This alert occurs when an application tries to invisibly connect to the internet. Invisible connection attempts may represent a risk of Trojan or spyware application.

In the example above, the executable 'tooleaky.exe' is attempting to use Internet Explorer to access the internet.



Internet Explorer is trying to **connect to the Internet.** What would you like to do?

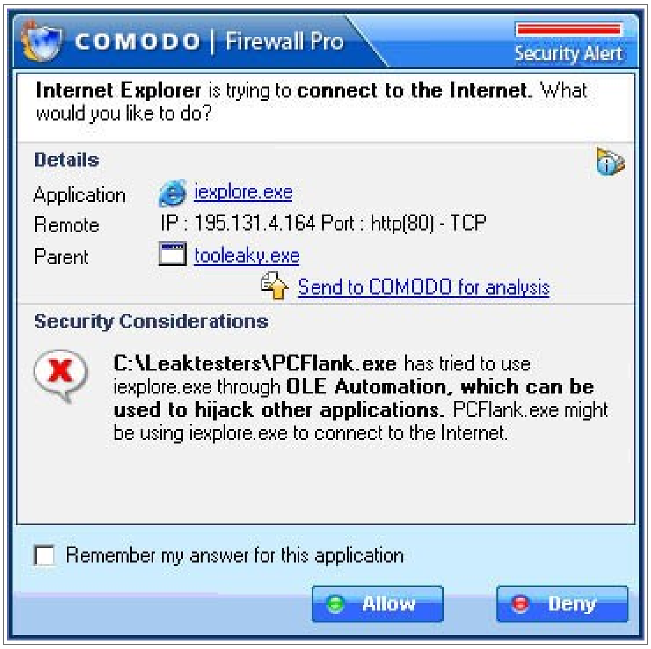
Details

Application iexplore.exe
Remote IP : 4.79.142.200 Port : http(80) - TCP
Parent tooleaky.exe

Security Considerations

iexplore.exe is an **invisible application.** Invisible applications connecting to the Internet could be a sign of trojan/spyware/virus activity. A **new parent application** has been detected for iexplore.exe. tooleaky.exe may be using iexplore.exe to connect to the Internet.

OLE Automation: This alert occurs when any application is deducted to occur by misuse of COM/OLE interfaces, which can hijack other applications.



Internet Explorer is trying to **connect to the Internet.** What would you like to do?

Details

Application iexplore.exe

Remote IP : 195.131.4.164 Port : http(80) - TCP

Parent tooleaky.exe

Send to COMODO for analysis

Security Considerations

C:\Leaktesters\PCFlank.exe has tried to use iexplore.exe through **OLE Automation, which can be used to hijack other applications.** PCFlank.exe might be using iexplore.exe to connect to the Internet.

□ Remember my answer for this application

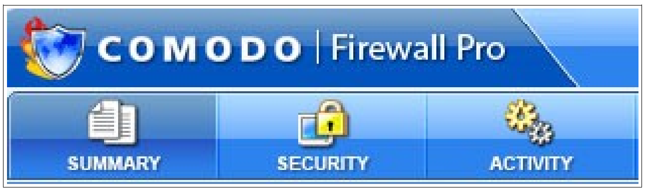
Firewall Summary

The Main Interface

After installation, Comodo Firewall Pro automatically protects any computer on which it is installed. You do not have to start the program to be protected.

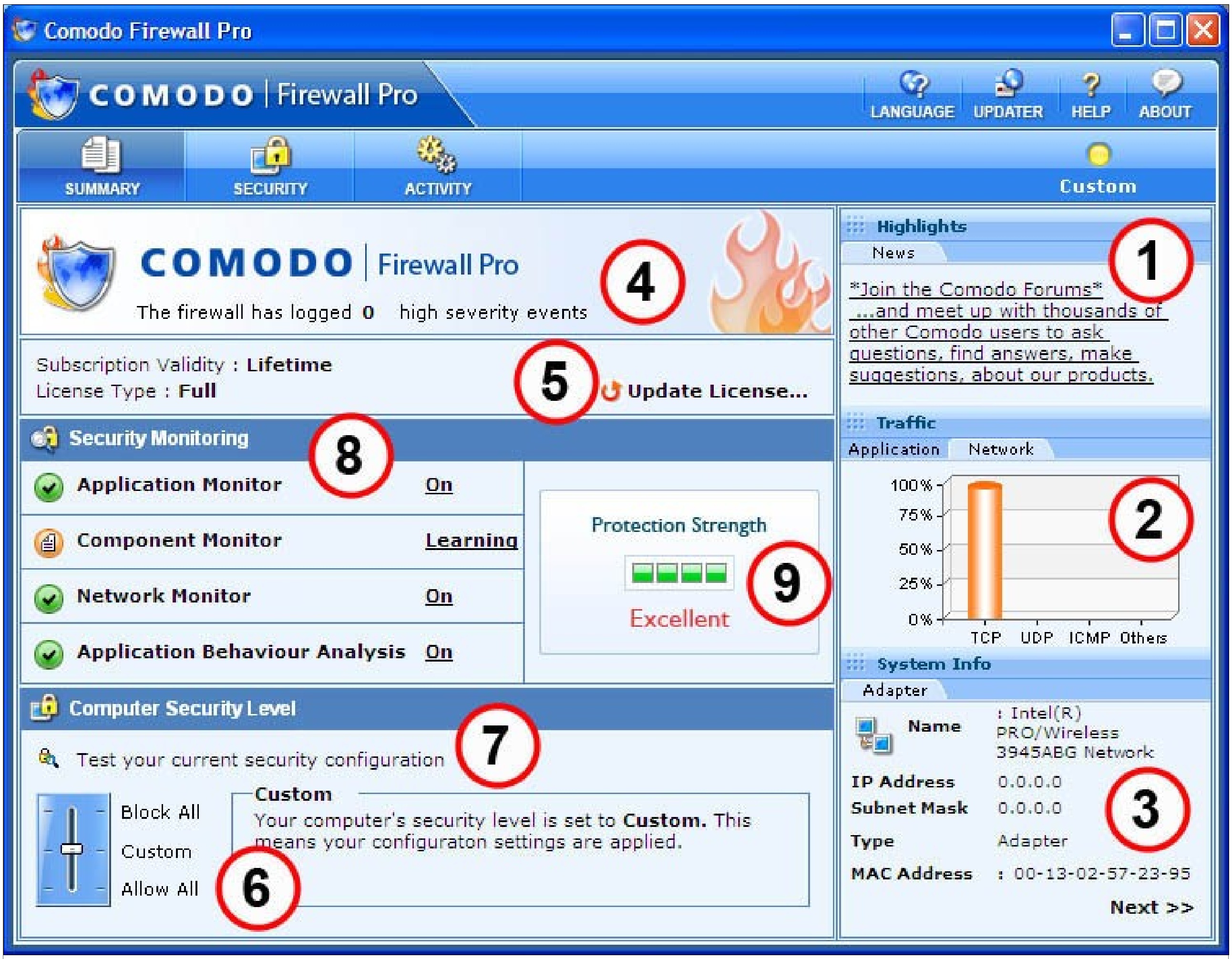
See Starting Comodo Firewall Pro if you are unsure of how to access the main interface.

The interface contains three main area indicated by the tabs at the top left hand of the interface- Summary, Security and Activity.



By default, the management interface displays the 'Summary' area information. You can also access this area at any time by selecting the 'Summary' tab as shown above.

The '**Summary**' area contains at-a-glance details of firewall settings and details.



The firewall has logged 0 high severity events

Subscription Validity : **Lifetime**
License Type : **Full**

Application Monitor On
Component Monitor Learning
Network Monitor On
Application Behaviour Analysis On

Test your current security configuration

Custom
Your computer's security level is set to **Custom.** This means your configuraton settings are applied.

Join the Comodo Forums ...and meet up with thousands of other Comodo users to ask questions, find answers, make suggestions, about our products.

Name	: Intel(R) PRO/Wireless 3945ABG Network
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Type	Adapter
MAC Address	: 00-13-02-57-23-95

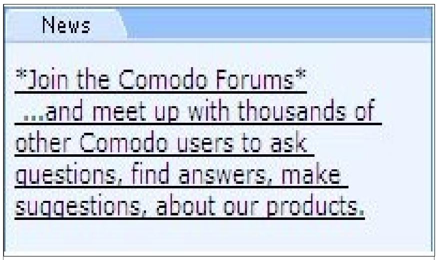
Figure: Comodo Firewall Summary

Highlights

The Highlights section displays information about Security Alerts and News related to Comodo Firewall Pro & latest Critical security updates. You can view information about News and Alerts by clicking on News and Alerts tabs in the Highlights section of the main Comodo Firewall Pro GUI.

News

This section contains direct news feeds from from the Comodo Server. You can also download the latest information about critical security updates and latest news about Comodo from the **News** section.



Join the Comodo Forums ...and meet up with thousands of other Comodo users to ask questions, find answers, make suggestions, about our products.

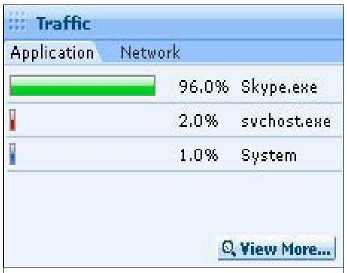
Figure: News

Traffic Info

Comodo Firewall Pro produces a Traffic history graph to give an overview of the last one minute of your traffic history in terms of the most used **Applications** and Network protocols.

Application

You can view the information about the most active applications in the last 1 minute based on the traffic used by the applications. The Application Traffic History graphs produce a real-time picture of the last one minute of your traffic in terms of the highest number of simultaneous open network connections since the program started.



🟩	96.0%	Skype.exe
🟥	2.0%	svchost.exe
▨	1.0%	System

Figure: Active Applications

Click ***View More*** to get more information about current active applications, the protocol being used, and the addresses or names of the connected computers. (This performs the same function as clicking 'Activity' at the top left hand of the main interface and takes you to the Connections screen).

Network

Comodo Firewall Pro maintains real-time network counters that track users' Internet usage. The detailed statistics include the information about the overall network protocol distribution, Network TCP, UDP and ICMP bytes sent and received. Click on the Network link under Traffic section to get the information.

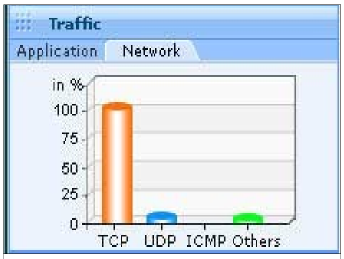


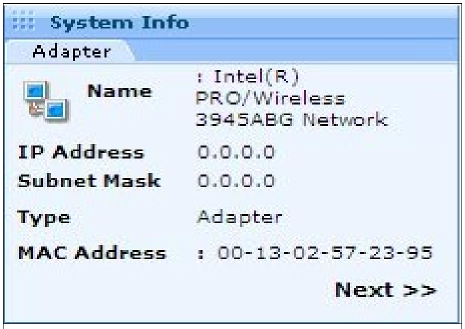
Figure: Network Traffic

The network traffic provides instant data, in percentage, about your incoming and outgoing network traffic.

System Info

The 'System' Info area of the summary screen contains details about the network adapters installed on your computer.

Adapters


System Info

Adapter

Name	: Intel(R) PRO/Wireless 3945ABG Network
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Type	Adapter
MAC Address	: 00-13-02-57-23-95

Figure: Network Adapter

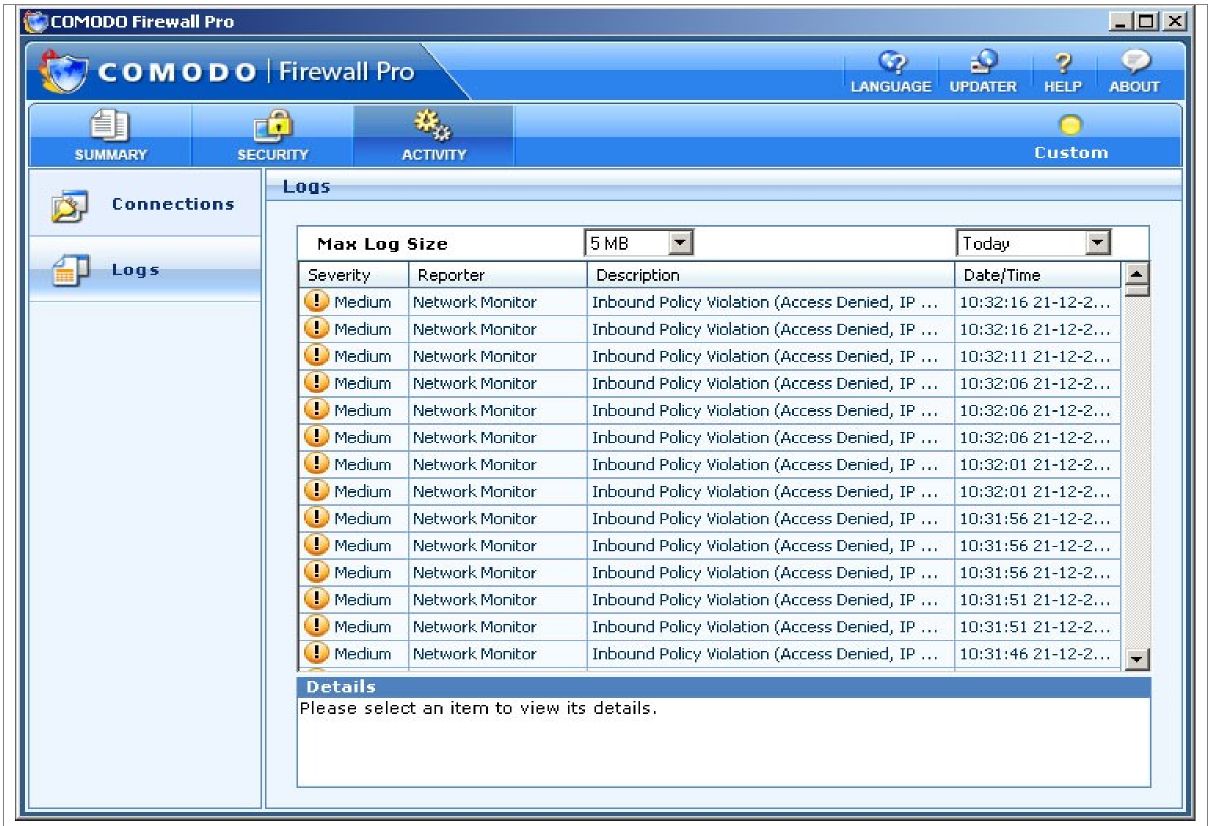
Comodo Firewall Pro detects all of the network adapters in your computer and provides you with a summary of the details of the network adapters in your system. A network adapter could be a modem, an Ethernet network card, a virtual VPN adapter, or a virtual PPPoE adapter (used for some DSL Connections).

Dial-up

If you are using a Dial-up coonection, then you can view the Dial-Up Adapter details by clicking ***Next***.

View Alerts

You can view information about the type of security alerts, the threat level and the communication that triggered this alert by clicking on the ***Logs*** tab in the Activity main screen.



Logs

Max Log Size: 5 MB | Today

Severity	Reporter	Description	Date/Time
Medium	Network Monitor	Inbound Policy Violation (Access Denied, IP ...	10:32:16 21-12-2...
Medium	Network Monitor	Inbound Policy Violation (Access Denied, IP ...	10:32:16 21-12-2...
Medium	Network Monitor	Inbound Policy Violation (Access Denied, IP ...	10:32:11 21-12-2...
Medium	Network Monitor	Inbound Policy Violation (Access Denied, IP ...	10:32:06 21-12-2...
Medium	Network Monitor	Inbound Policy Violation (Access Denied, IP ...	10:32:06 21-12-2...
Medium	Network Monitor	Inbound Policy Violation (Access Denied, IP ...	10:32:06 21-12-2...
Medium	Network Monitor	Inbound Policy Violation (Access Denied, IP ...	10:32:01 21-12-2...
Medium	Network Monitor	Inbound Policy Violation (Access Denied, IP ...	10:32:01 21-12-2...
Medium	Network Monitor	Inbound Policy Violation (Access Denied, IP ...	10:31:56 21-12-2...
Medium	Network Monitor	Inbound Policy Violation (Access Denied, IP ...	10:31:56 21-12-2...
Medium	Network Monitor	Inbound Policy Violation (Access Denied, IP ...	10:31:56 21-12-2...
Medium	Network Monitor	Inbound Policy Violation (Access Denied, IP ...	10:31:51 21-12-2...
Medium	Network Monitor	Inbound Policy Violation (Access Denied, IP ...	10:31:51 21-12-2...
Medium	Network Monitor	Inbound Policy Violation (Access Denied, IP ...	10:31:46 21-12-2...

Details

Please select an item to view its details.

Figure: Alerts Reports

Max Log Size

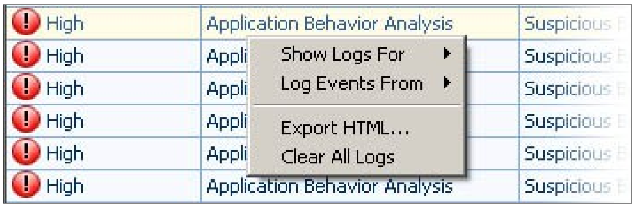
Comodo stores the events reported by the firewall engine in the log. You can view the details of the alerts triggered by the possible attacks on your computer. The events are reported and stored in HTML format. You can reduce the maximum size of the log file from 5 MB , 10, MB, 15 MB, 25 MB , 50 MB and 100 MB by selecting the File size from the ***Maximum Log size*** Drop down menu.

Columns Description:

1. The First Column ***(Severity)*** represents the threat level of an attack: High, Medium and Low. High severity alerts are very serious security risks like DOS and Port Scan attacks and the firewall goes into emergency to temporarily block incoming traffic. Medium and Low severity alerts are not so serious and are caused by transgression of one or more Network Control rules.
2. The Second Column ***(Reporter)*** states which subsystem generated the attack report. (Application Monitor, Network Monitor, Component Monitor or Application Behaviour Monitor).
3. The Third Column (***Description)*** represents the nature of the logged alert. For example , alerts could be caused by policy violation caused by transgressing a Network Control Rule; DOS (Denial Of Service) attack or TCP/UDP Port Scan .
4. The Fourth Column **(Date & Time)** represents the date and time when the alerts were triggered.

Context Sensitive Menu

Right clicking on the alert list reveals a context sensitive menu containing futher log options.



! High	Application Behavior Analysis	Suspicious
! High	Appli	Suspicious
! High	Appli	Suspicious
! High	Appli	Suspicious
! High	Appli	Suspicious
! High	Application Behavior Analysis	Suspicious

Show Logs For - The user can choose to view logs of all alerts from Today, Last 7 days or Last 30 days. The default is to show today's alerts only.

Log Events From - There are four seperate components of Comodo Firewall that have the potential to populate the 'Log' area with the alerts they generate. This entry lets the user change which events are recorded in the logs according to the component that generated them. By default, alerts generated by all four components are recorded. Comodo advise users to leave this setting at the default.

Export HTML.... Users can export a more detailed HTML copy of the logs to local or network drives. This is very useful for records and troubleshooting purposes. Click the 'Export HTML...' entry, choose a filename and destination and click 'Save'

Clear All Logs: Empties the current view

Types of Alerts

There are three types of alerts based on their severity levels : High, Medium and Low.

High, Medium and Low Severity Alerts :

High Severity Alerts are represented by a Red icon !. High Severity alerts are generated by DOS (Denial of Service) attacks, Port Scan, Trojan Probe attacks and when application monitor detects a 'leak'.

When a high severity alert is detected, the Firewall goes into emergency mode. The firewall will stay in emergency mode for the duration set by user i.e *time to stay in emergency mode*, by default, the duration is set to 120 seconds. In the emergency mode, all inbound traffic is blocked except those previously established and active connections. However, all outbound traffic is still allowed.

Medium severity alerts are represented by an Orange icon !

Low severity alerts are represented by a Green icon !.

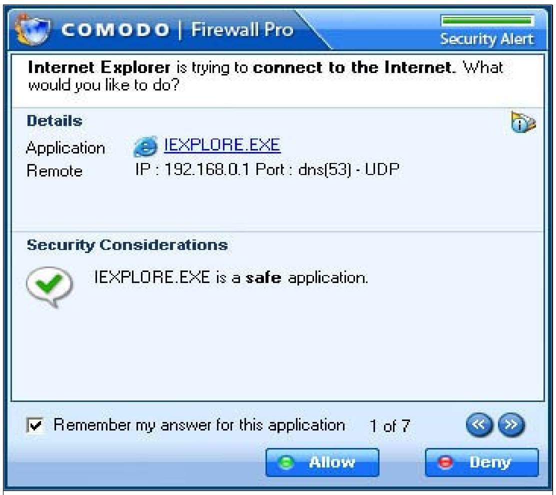
Medium and Low severity alerts are caused by violation of network control rules.

Alert Description :

You can view details about a generated alert by selecting it and clicking on the Description tab . You will get information about the nature of attack, Source IP, Destination IP and cause which triggered the alert.

Alert

When Comodo Firewall intercepts any unknown program or a program not matching the set rules, you will be prompted by the generation of a Alert Pop-Up window.



COMODO | Firewall Pro
Security Alert

Internet Explorer is trying to **connect to the Internet**. What would you like to do?

Details

Application IEXPLORE.EXE
Remote IP : 192.168.0.1 Port : dns(53) - UDP

Security Considerations

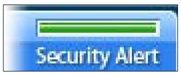
IEXPLORE.EXE is a **safe** application.

☑ Remember my answer for this application 1 of 7

Figure: Alert Pop-Up

The Alert includes information like name of Application which triggered the alert, the Parent Application , the Protocol used by the Application, its IP address and its Port Number.

The top right corner of the pop up also shows the Security Alert Severity Level. The colour assignations correspond to those outlined above in ***High, Medium*** and ***Low Severity Alerts.***



For example, pop window shown above indicates a green severity security level.
This is because Internet Explorer is considered a safe application. Quickly glancing at the alert level indicator provides a quick way to determine whether an application or activity should concern the user.

Details

Contains:

- The application name
- The IP address of the site it is attempting to connect to
- The port it is using to make the connection
- The protocol it is using to facilitate the connect

Security Considerations

This area provides a consise, at a glance summary of the security risk involved with allowing this application to access the internet.

Choose options

Once you understand the risk, you can respond in the following ways :

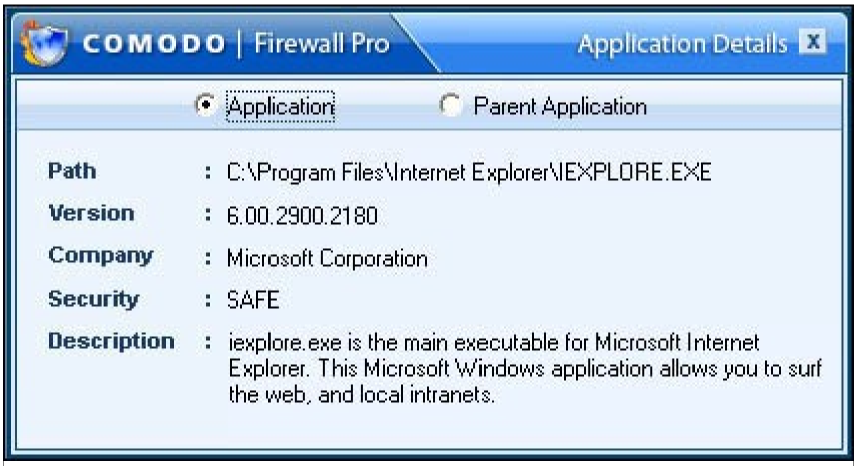
Remember my answer for this application: check this box to instruct the Firewall not to generate an alert again if the parameters of the application are the same.

Allow - allows the current instance of the application to access the internet according to the delinated parameters

Deny - Blocks the application from accessing the internet

More Details

If you are unsure about the application, you can view more information about the application by clicking *More Details* tab so that you can decide what to do. When you click More Details, a Pop-up window will appear a brief information about the application.

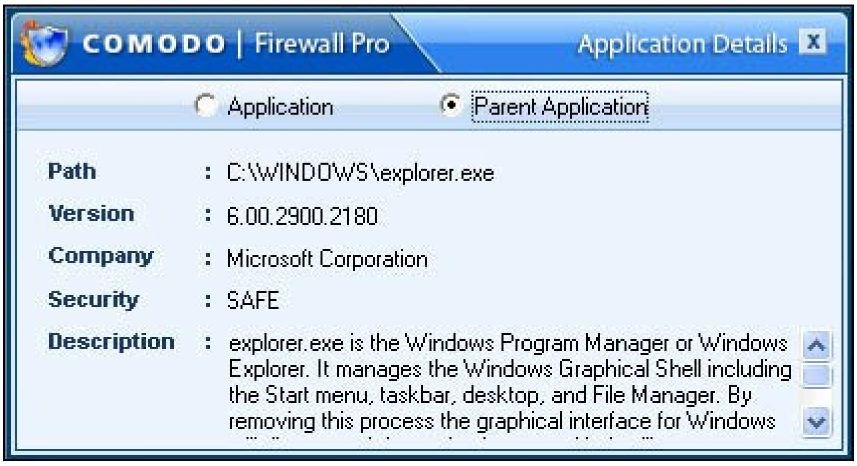


● Application ○ Parent Application

Path : C:\Program Files\Internet Explorer\IEXPLORE.EXE
Version : 6.00.2900.2180
Company : Microsoft Corporation
Security : SAFE
Description : iexplore.exe is the main executable for Microsoft Internet Explorer. This Microsoft Windows application allows you to surf the web, and local intranets.

Figure: More Details About The Application

Selecting the 'Parent Application' radio button enables the user to view information about the application that originally caused the child application to try to access the internet. In this case, Explorer.exe commanded Internet Explorer.exe to access the internet. 'Explorer.exe' is therefore the parent application to 'Internet Explorer.exe'.



○ Application ● Parent Application

Path : C:\WINDOWS\explorer.exe
Version : 6.00.2900.2180
Company : Microsoft Corporation
Security : SAFE
Description : explorer.exe is the Windows Program Manager or Windows Explorer. It manages the Windows Graphical Shell including the Start menu, taskbar, desktop, and File Manager. By removing this process the graphical interface for Windows

Update License

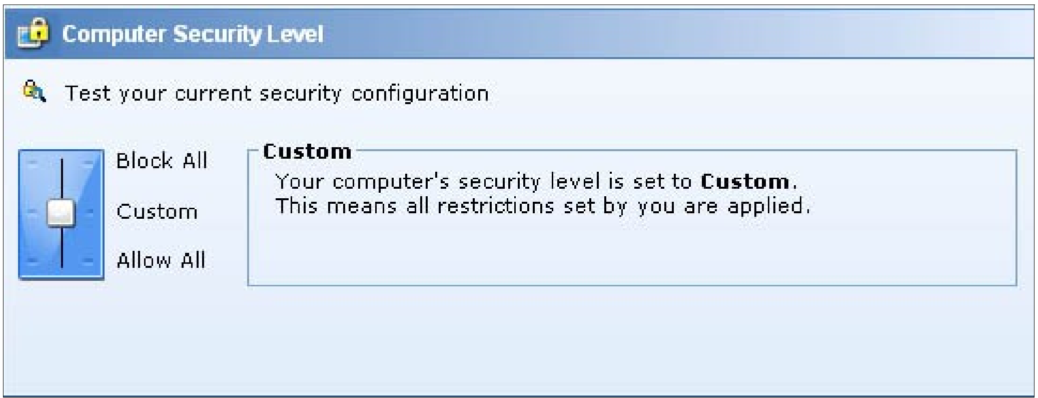
You can update the Comodo Firewall Pro license by clicking on the ***Update License*** tab in the main Comodo Firewall Pro GUI and the license wizard will open to guide you through the process of updating your license. After activation of your license, the summary screen will no longer show this link.

Computer Security Level

Comodo Firewall Pro allows you to customize firewall security by using the Computer Security Level slider to change preset security levels. The Computer Security Level Slider allows you to select Block All, Custom or Allow All security settings by adjusting the slider to change the security levels.

To Change the Computer Security Level slider:

1. Open Comodo Firewall Pro GUI.
2. In the Computer Security Level, adjust the slider to Block All, Custom or Allow All.



Computer Security Level

Test your current security configuration

Custom
Your computer's security level is set to **Custom**.
This means all restrictions set by you are applied.

Figure: Computer Level Security Slider

You can adjust the slider to the Computer Security Level you want:

► **Block All**: The firewall blocks everything irrespective of the restrictions set by the user.

► **Custom**: Custom security configuration created by the user is applied.

► **Allow All**: Disables the firewall and makes it inactive. All incoming and outgoing connections are allowed irrespective of the restrictions set by the user.

The security level chosen by you will also appear in the form of a coloured ball icon on the top-right hand corner of the Comodo Firewall Pro GUI: A **Red** icon represents 'Block All' Security , an **Yellow** icon represents Custom Level Security and a **Green** Icon represents a 'Allow All' security.

Clicking 'Test your current security configuration' contacts the Comodo HackerGuardian website (www.hackerguardian.com).

HackerGuardian vulnerability scans conduct in depth testing of your computer and network to identify potential security holes.

Sign up for a 'Free Scan' to find out how well defended your system is against hackers.

Test Security Configuration

You can check your current security configuration and see how vulnerable your system is for outside attack by clicking the current security configuration icon 🔍. The user will be directed to **http://www.hackerguardian.com/** a Comodo site which let's you check your server vulnerabilities.

Security Monitoring

The **Security Monitoring Section** section provides shortcuts to tasks in the Security section of the firewall. These sections allow you to configure Firewall operations and settings administrating

Application Monitior - Shortcut to the Application Monitoring Section of Security. 2 modes of operation, ON or OFF
Component Monitor - Shortcut to the Component Monitor Section of Security. 3 modes of operation ON, OFF or LEARN MODE

Network Monitor - Shortcut to the Network Monitoring Section of Security. 2 modes of operation ON and OFF
Application Behavior Analysis - Shortcut to the Advanced Section of Security. 2 modes of operation ON and OFF

Protection Strength

There are five levels of protection strength. Comodo Firewall Pro determines the protection strength based on the ON or OFF attributes for each of the sections in the Security Monitoring section above. The five levels are Excellent - Good - Fair - Poor - Bad. The default settings of Application Monitor (ON), Component Monitor (Learn Mode), Network Monitor (ON) and Application Behaviour Analysis (ON) produce a default Protection Strength of 'Excellent'

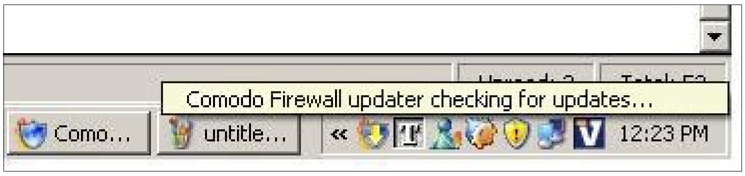
Updater

The **Comodo Firewall Pro Updater** will download Manual or Automatic updates only if your computer is connected to the Internet. If Internet connection is unavailable, the updating process will not start.

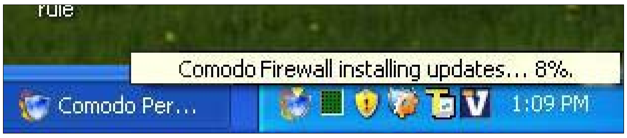
There are two types of Updater. These are: **Automatic Updater | Manual Updater.**

Automatic Updater

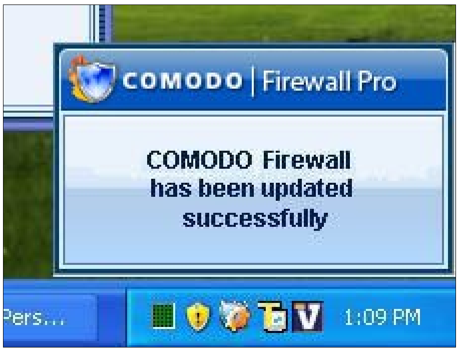
The 'Automatic updater' module checks for update availability once a day. As it is checking it shows a flashing icon in system tray as shown below:


Comodo Firewall updater checking for updates...

If updates are available the message box is displayed otherwise not and it checks again next day. To download the updates click **Yes** else **No**. If you click **No** the updates would not take place. After updates are installed, a pop-up


Comodo Firewall installing updates... 8%.

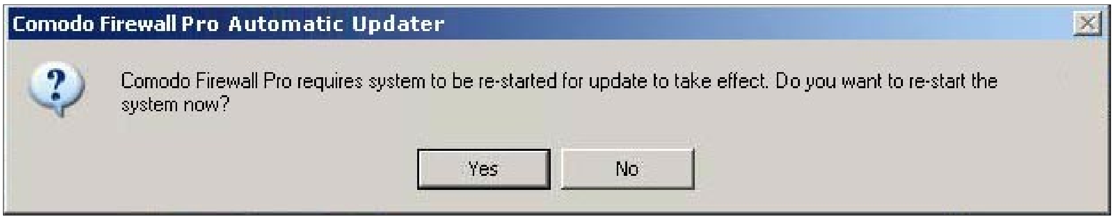
emerges from the system tray as shown below:


COMODO | Firewall Pro

COMODO Firewall has been updated successfully

After the installation process is completed you will need to re-start your computer for the changes to take effect.

Click 'Yes' to re-start immediately or 'No' to re-start at a later time.



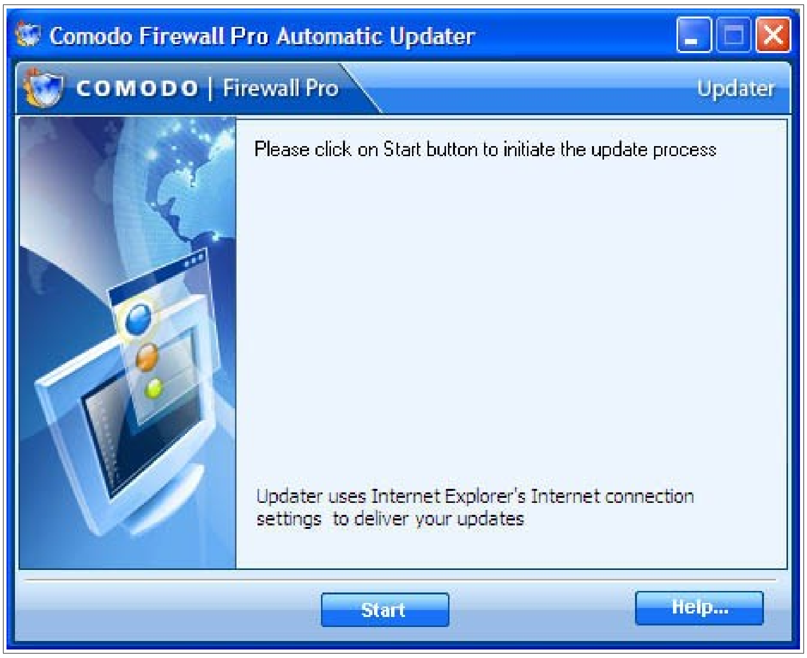
Comodo Firewall Pro Automatic Updater

Comodo Firewall Pro requires system to be re-started for update to take effect. Do you want to re-start the system now?

Manual Updater

Manual updates can be downloaded and installed at any time by clicking the 'Updater' button in the top right hand corner of the firewall interface:

If updates are available, the following screen appears.

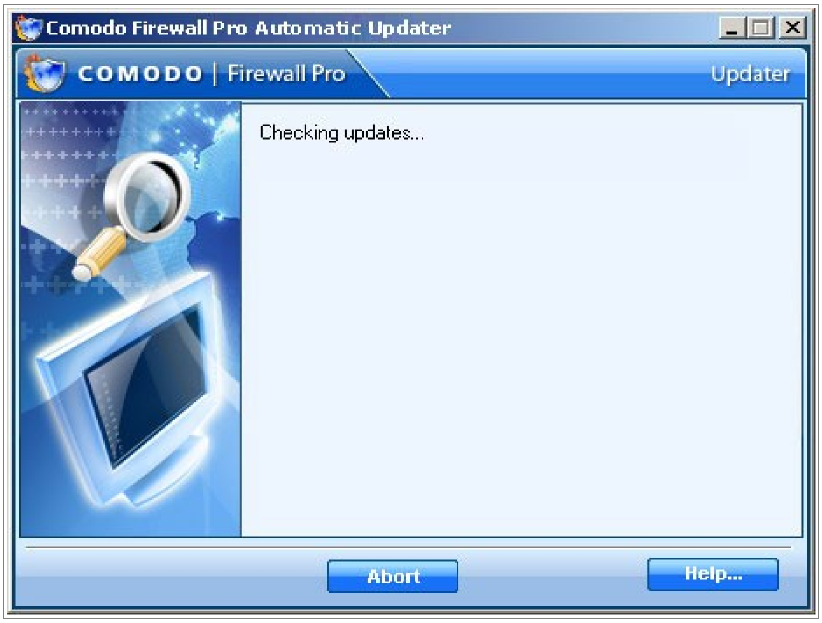


Comodo Firewall Pro Automatic Updater

Please click on Start button to initiate the update process

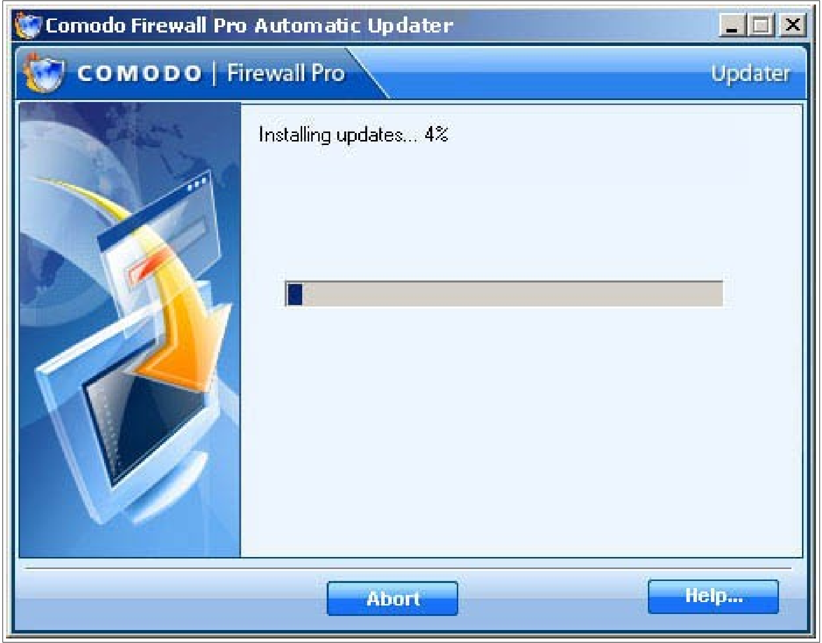
Updater uses Internet Explorer's Internet connection settings to deliver your updates

To intiate the update process click on the **Start** button. If you want to initiate the updates later, click on the **Abort** button to leave the Updater wizard.



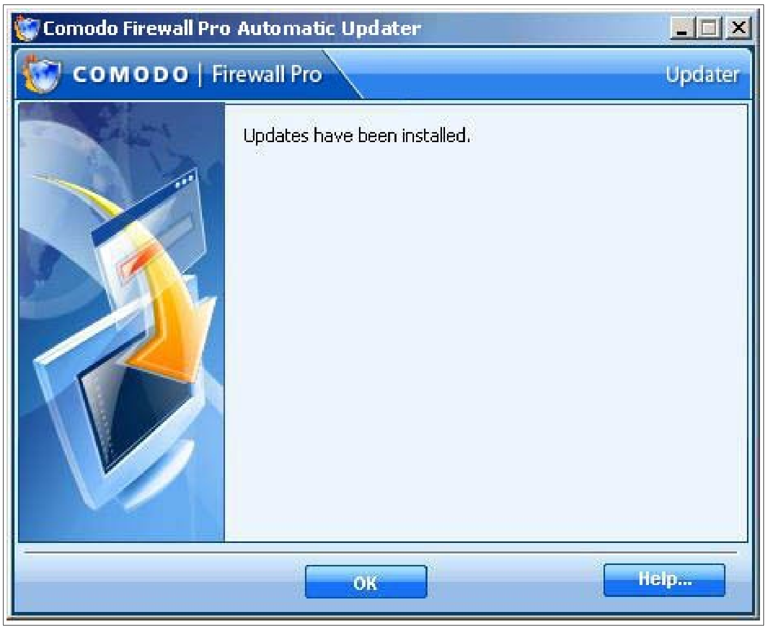
Checking updates...

If the software finds any new updates it will start installing.



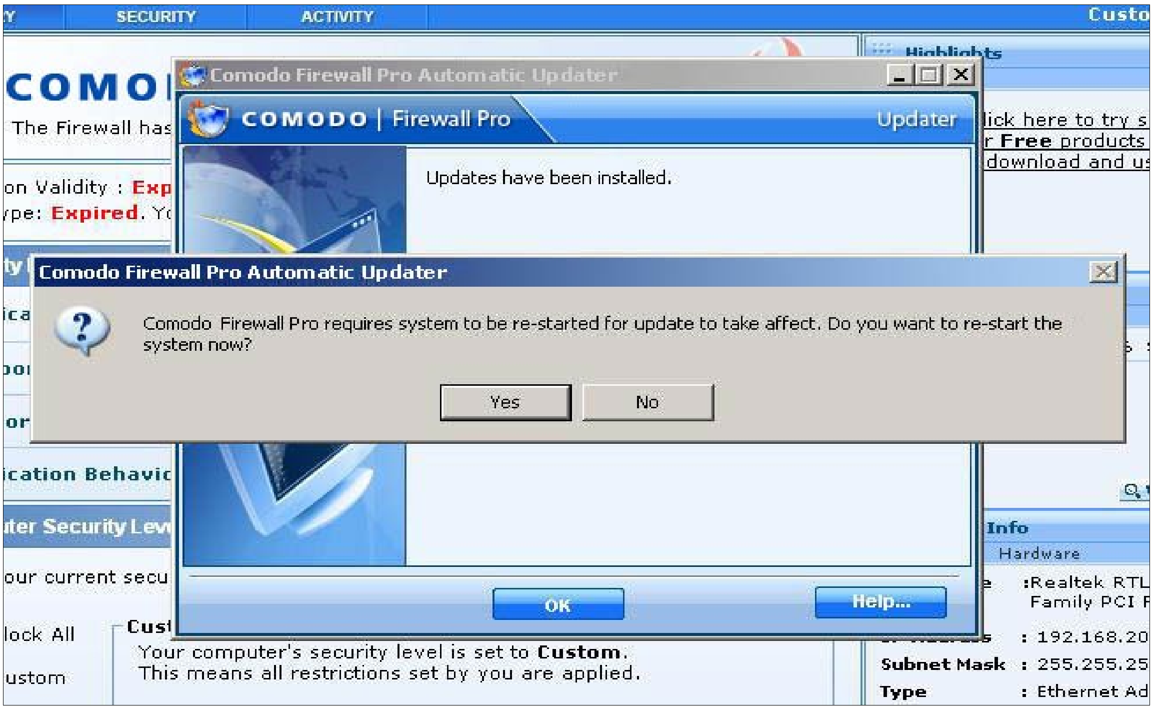
Installing updates... 4%

Once the installation of updates is finished, the message **Updates have been installed** will appear on the screen.



Updates have been installed.

After the installation process is completed, Click **OK**. It will request you to restart the system.



Updates have been installed.

Comodo Firewall Pro Automatic Updater

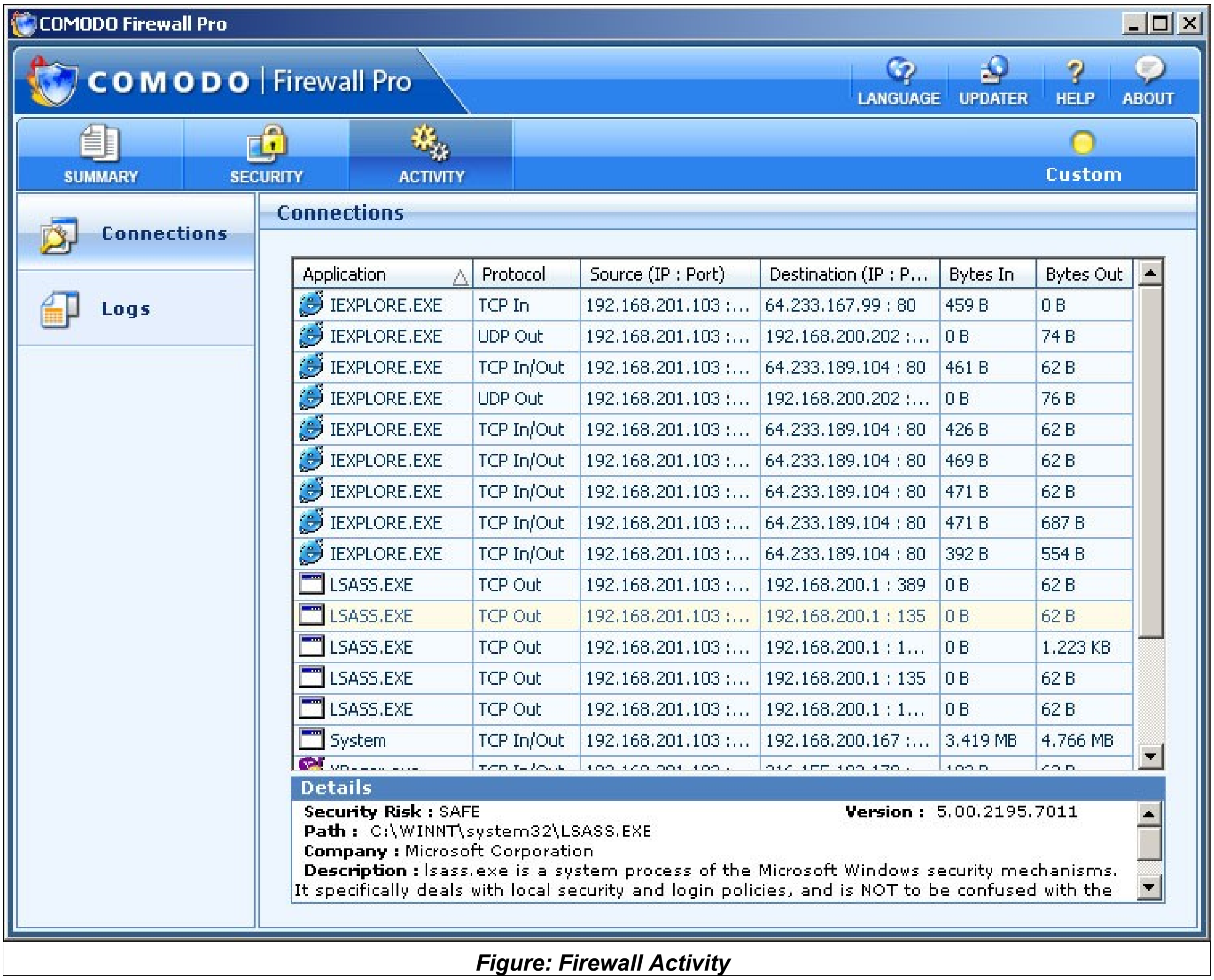
Comodo Firewall Pro requires system to be re-started for update to take affect. Do you want to re-start the system now?

Your computer's security level is set to **Custom**.
This means all restrictions set by you are applied.

Click **Yes** to reboot the system now or **No** to reboot at a later time.

Firewall Activity

Comodo Firewall Pro records information about all application and network connections, actions that the firewall has taken, and any alerts that have been triggered. The ***Activity*** section includes details about active ***Connections*** and the ***Logs*** section includes customized information about triggered Security alerts.



Connections

Application	Protocol	Source (IP : Port)	Destination (IP : P...	Bytes In	Bytes Out
IEXPLORE.EXE	TCP In	192.168.201.103 :...	64.233.167.99 : 80	459 B	0 B
IEXPLORE.EXE	UDP Out	192.168.201.103 :...	192.168.200.202 :...	0 B	74 B
IEXPLORE.EXE	TCP In/Out	192.168.201.103 :...	64.233.189.104 : 80	461 B	62 B
IEXPLORE.EXE	UDP Out	192.168.201.103 :...	192.168.200.202 :...	0 B	76 B
IEXPLORE.EXE	TCP In/Out	192.168.201.103 :...	64.233.189.104 : 80	426 B	62 B
IEXPLORE.EXE	TCP In/Out	192.168.201.103 :...	64.233.189.104 : 80	469 B	62 B
IEXPLORE.EXE	TCP In/Out	192.168.201.103 :...	64.233.189.104 : 80	471 B	62 B
IEXPLORE.EXE	TCP In/Out	192.168.201.103 :...	64.233.189.104 : 80	471 B	687 B
IEXPLORE.EXE	TCP In/Out	192.168.201.103 :...	64.233.189.104 : 80	392 B	554 B
LSASS.EXE	TCP Out	192.168.201.103 :...	192.168.200.1 : 389	0 B	62 B
LSASS.EXE	TCP Out	192.168.201.103 :...	192.168.200.1 : 135	0 B	62 B
LSASS.EXE	TCP Out	192.168.201.103 :...	192.168.200.1 : 1...	0 B	1.223 KB
LSASS.EXE	TCP Out	192.168.201.103 :...	192.168.200.1 : 135	0 B	62 B
LSASS.EXE	TCP Out	192.168.201.103 :...	192.168.200.1 : 1...	0 B	62 B
System	TCP In/Out	192.168.201.103 :...	192.168.200.167 :...	3.419 MB	4.766 MB

Details

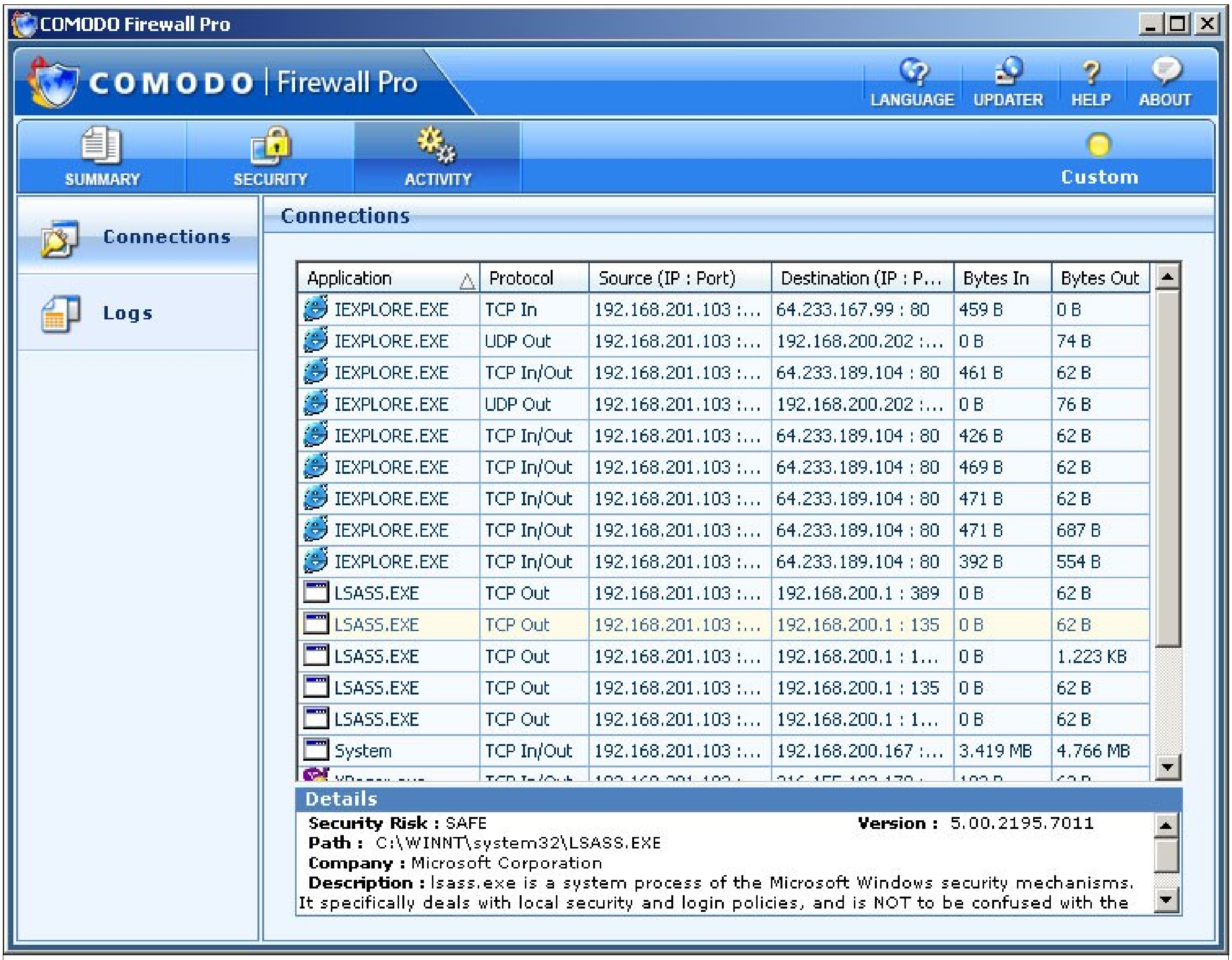
Security Risk : SAFE **Version :** 5.00.2195.7011
Path : C:\WINNT\system32\LSASS.EXE
Company : Microsoft Corporation
Description : lsass.exe is a system process of the Microsoft Windows security mechanisms. It specifically deals with local security and login policies, and is NOT to be confused with the

Figure: Firewall Activity

Connections

A list of active connections on the network and the connection parameters used in the Connections section of Activity Report. Comodo Firewall Pro records information about all application and network connections, actions that the firewall has taken, and any alerts that have been triggered.

Select the ***Connections*** tab in the Activity Overview section to view the list of active connections on the network and the connection parameters used by individual applications.



Connections

Application	Protocol	Source (IP : Port)	Destination (IP : P...	Bytes In	Bytes Out
IEXPLORE.EXE	TCP In	192.168.201.103 :...	64.233.167.99 : 80	459 B	0 B
IEXPLORE.EXE	UDP Out	192.168.201.103 :...	192.168.200.202 :...	0 B	74 B
IEXPLORE.EXE	TCP In/Out	192.168.201.103 :...	64.233.189.104 : 80	461 B	62 B
IEXPLORE.EXE	UDP Out	192.168.201.103 :...	192.168.200.202 :...	0 B	76 B
IEXPLORE.EXE	TCP In/Out	192.168.201.103 :...	64.233.189.104 : 80	426 B	62 B
IEXPLORE.EXE	TCP In/Out	192.168.201.103 :...	64.233.189.104 : 80	469 B	62 B
IEXPLORE.EXE	TCP In/Out	192.168.201.103 :...	64.233.189.104 : 80	471 B	62 B
IEXPLORE.EXE	TCP In/Out	192.168.201.103 :...	64.233.189.104 : 80	471 B	687 B
IEXPLORE.EXE	TCP In/Out	192.168.201.103 :...	64.233.189.104 : 80	392 B	554 B
LSASS.EXE	TCP Out	192.168.201.103 :...	192.168.200.1 : 389	0 B	62 B
LSASS.EXE	TCP Out	192.168.201.103 :...	192.168.200.1 : 135	0 B	62 B
LSASS.EXE	TCP Out	192.168.201.103 :...	192.168.200.1 : 1...	0 B	1.223 KB
LSASS.EXE	TCP Out	192.168.201.103 :...	192.168.200.1 : 135	0 B	62 B
LSASS.EXE	TCP Out	192.168.201.103 :...	192.168.200.1 : 1...	0 B	62 B
System	TCP In/Out	192.168.201.103 :...	192.168.200.167 :...	3.419 MB	4.766 MB

Details

Security Risk : SAFE **Version :** 5.00.2195.7011
Path : C:\WINNT\system32\LSASS.EXE
Company : Microsoft Corporation
Description : lsass.exe is a system process of the Microsoft Windows security mechanisms. It specifically deals with local security and login policies, and is NOT to be confused with the

Figure: List of Active Connections

Columns Description:

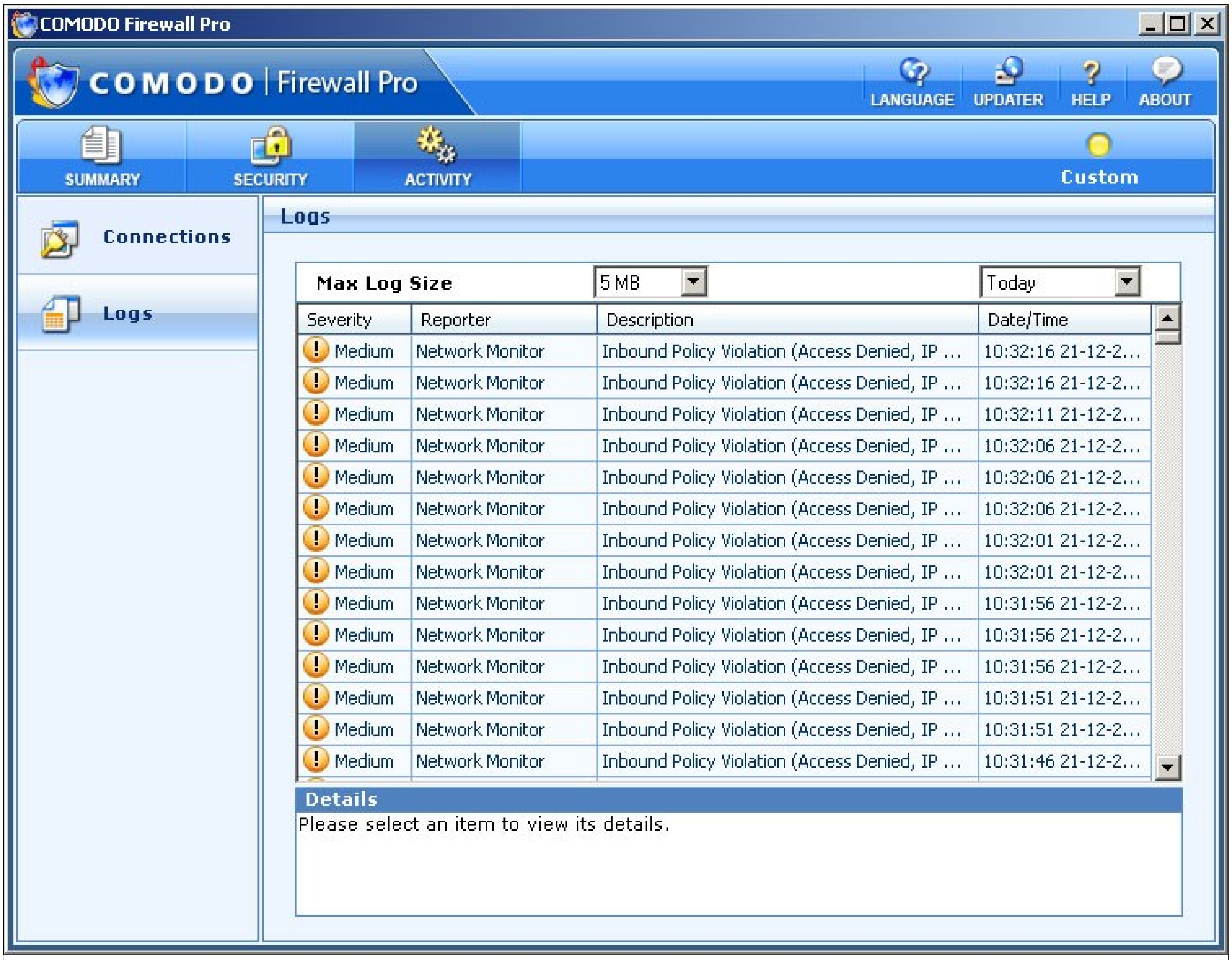
- The First Column ***(Application)*** represents each application's icon and name (description) — if the application has no icon, the default system icon for executable files will be used; if no description (name) is available, the name of the file without the extension will be displayed.
- The Second Column ***(Protocol)*** represents the Protocols, usually TCP, UDP or Both, used by the applications.
- The Third Column ***Source (IP : Port)*** represents the ports used by the individual applications.
- The Fourth Column ***Destination (IP : Port)*** represents IP Address of the application. In case the application is waiting for communication and the port is open, it is described as ‘Listening’.
- The Fifth Column ***(Bytes In)*** represents the Total extent of incoming (In) data within the particular connection in Bytes.
- The Sixth Column **(Bytes Out)** represents the Total extent of Outgoing (Out) data within the particular connection in Bytes.

Details

You can view additional information about individual applications by selecting an application in column 1. The *Details* panel at the foot of the interface displays in depth information about the particular application. In the example above, you can view Application information like Application name (c:\Program Files\Skype\Skype.exe) , Company, Description (a concise description of the progam polled from the application database) Version and Security Risk (SAFE).

Logs

You can view information about the type of security alerts, the threat level and the communication that triggered this alert by clicking on the ***Logs*** tab in the Activity main screen.



Max Log Size: 5 MB — Today

Severity	Reporter	Description	Date/Time
Medium	Network Monitor	Inbound Policy Violation (Access Denied, IP ...	10:32:16 21-12-2...
Medium	Network Monitor	Inbound Policy Violation (Access Denied, IP ...	10:32:16 21-12-2...
Medium	Network Monitor	Inbound Policy Violation (Access Denied, IP ...	10:32:11 21-12-2...
Medium	Network Monitor	Inbound Policy Violation (Access Denied, IP ...	10:32:06 21-12-2...
Medium	Network Monitor	Inbound Policy Violation (Access Denied, IP ...	10:32:06 21-12-2...
Medium	Network Monitor	Inbound Policy Violation (Access Denied, IP ...	10:32:06 21-12-2...
Medium	Network Monitor	Inbound Policy Violation (Access Denied, IP ...	10:32:01 21-12-2...
Medium	Network Monitor	Inbound Policy Violation (Access Denied, IP ...	10:32:01 21-12-2...
Medium	Network Monitor	Inbound Policy Violation (Access Denied, IP ...	10:31:56 21-12-2...
Medium	Network Monitor	Inbound Policy Violation (Access Denied, IP ...	10:31:56 21-12-2...
Medium	Network Monitor	Inbound Policy Violation (Access Denied, IP ...	10:31:56 21-12-2...
Medium	Network Monitor	Inbound Policy Violation (Access Denied, IP ...	10:31:51 21-12-2...
Medium	Network Monitor	Inbound Policy Violation (Access Denied, IP ...	10:31:51 21-12-2...
Medium	Network Monitor	Inbound Policy Violation (Access Denied, IP ...	10:31:46 21-12-2...

Details

Please select an item to view its details.

Figure: Alerts Reports

Max Log Size

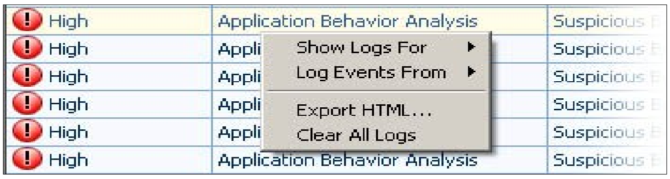
Comodo stores the events reported by the firewall engine in the log. You can view the details of the alerts triggered by the possible attacks on your computer. The events are reported and stored in HTML format. You can reduce the maximum size of the log file from 5 MB , 10, MB, 15 MB, 25 MB , 50 MB and 100 MB by selecting the File size from the ***Maximum Log size*** Drop down menu.

Columns Description:

1. The First Column ***(Severity)*** represents the threat level of an attack: High, Medium and Low. High severity alerts are very serious security risks like DOS and Port Scan attacks and the CPF goes into emergency to temporarily blocks incoming traffic. Medium and Low severity alerts are not so serious and are caused by Network Control rules.
2. The Second Column ***(Reporter)*** represents the subsystems like Application Control engine or Network Control Engine which generated the attack reports.
3. The Third Column (***Description)*** represents the nature of attack , for example , attack types could be policy violation caused by a Control Rule , DOS (Denial Of Service) attack or TCP/UDP Port Scan .
4. The Fourth Column **(Date & Time)** represents the date and time when the alerts were triggered.

Context Sensitive Menu

Right clicking on the alert list reveals a context sensitive menu containing further log options.



High	Application Behavior Analysis	Suspicious
High	Appli	Suspicious
High	Appli	Suspicious
High	Appli	Suspicious
High	Appli	Suspicious
High	Application Behavior Analysis	Suspicious

Show Logs For - The user can choose to view logs of all alerts from Today, Last 7 days or Last 30 days. The default is to show today's alerts only.

Log Events From - There are four separate components of Comodo Firewall Pro that have the potential to populate the 'Log' area with the alerts they generate. This entry lets the user change which events are recorded in the logs according to the component that generated them. By default, alerts generated by all four components are recorded. Comodo advise users to leave this setting at the default.

Export HTML.... - Users can export a more detailed HTML copy of the logs to local or network drives. This is very useful for records and troubleshooting purposes. Click the 'Export HTML...' entry, choose a filename and destination and click 'Save'.

Clear All Logs - Empties the current view.

Types of Alerts

There are three types of alerts based on their severity levels: High, Medium and Low.

High, Medium and Low Severity Alerts:

High Severity Alerts are represented by a Red icon❗. High Severity alerts are generated by DOS (Denial of Service) attacks, Port Scan, Trojan Probe attacks and when application monitor detects a 'leak'.
When a high severity alert is detected , the firewall goes into emergency mode. The firewall will stay in emergency mode for the duration set by the user. This duration, set by default to 120 seconds, can be configured in the Intrusion Detection tab in 'Advanced Configuration. Whilst in emergency mode, all inbound traffic is blocked except those previously established and active connections. However, all outbound traffic is still allowed.

Medium severity alerts are represented by an Orange icon ❗

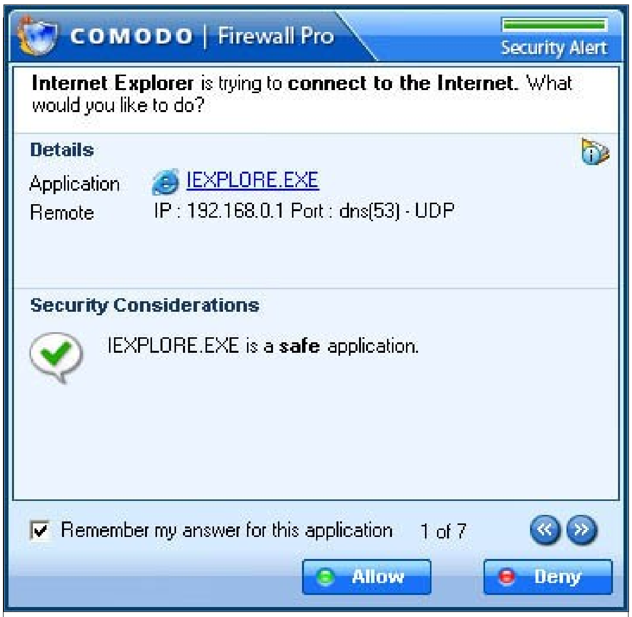
Low severity alerts are represented by a Green icon ❗.
Medium and Low severity alerts are caused by violation of network control rules.

Alert Description:

You can view details about a generated alert by selecting it and clicking on the Description tab . You will get information about the nature of attack, Source IP, Destination IP and cause which triggered the alert.

Alert

When Comodo Firewall Pro intercepts any unknown program or a program not matching the set rules, you will be prompted by the generation of a Alert window.



Internet Explorer is trying to **connect to the Internet**. What would you like to do?

Details

Application IEXPLORE.EXE
Remote IP : 192.168.0.1 Port : dns(53) - UDP

Security Considerations

IEXPLORE.EXE is a **safe** application.

☑ Remember my answer for this application 1 of 7

Figure: Alert Pop-Up

The Alert includes information like name of **Application** which triggered the alert, the **Parent Application**, the Protocol used by the Application, its IP address and its Port Number.
The top right corner of the pop up also shows the Security Alert Severity Level. The colour assignations correspond to those outlined above in High, Medium and Low Severity Alerts.

For example, pop window shown above indicates a green severity security level:

This is because Internet Explorer is considered a safe application. Quickly glancing at the alert level indicator provides a quick way to determine whether an application or activity should concern the user.

Details

Contains:

- The application name
- The IP address of the site it is attempting to connect to
- The port it is using to make the connection
- The protocol it is using to facilitate the connect

Security Considerations

This area provides a consise, at a glance summary of the security risk involved with allowing this application to access the internet.

Choose options

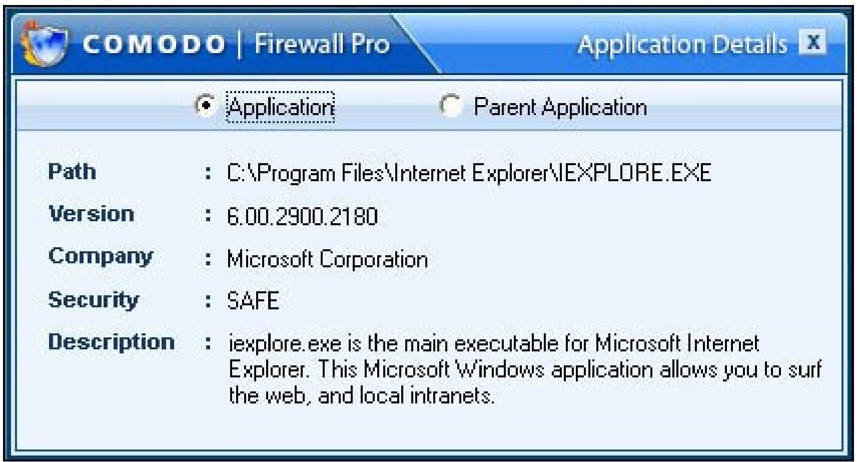
Once you understand the risk, you can respond in the following ways :
Remember my answer for this application: check this box to instruct the Firewall not to generate an alert again if the parameters of the application are the same.

Allow - allows the current instance of the application to access the internet according to the declinated parameters.

Deny - Blocks the application from accessing the internet

More Details

If you are unsure about the application, you can view more information about the application by clicking the icon at the top of any alert:



● Application ○ Parent Application

Path : C:\Program Files\Internet Explorer\IEXPLORE.EXE

Version : 6.00.2900.2180

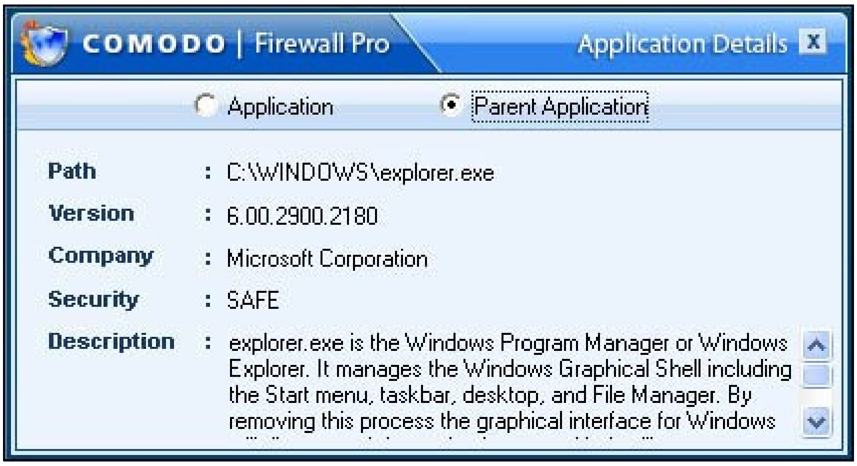
Company : Microsoft Corporation

Security : SAFE

Description : iexplore.exe is the main executable for Microsoft Internet Explorer. This Microsoft Windows application allows you to surf the web, and local intranets.

Figure: More Details About The Application

Selecting the 'Parent Application' radio button enables the user to view information about the application that originally caused the child application to try to access the internet. In this case, Explorer.exe commanded Internet Explorer.exe to access the internet. 'Explorer.exe' is therefore the parent application to 'Internet Explorer.exe'.



○ Application ● Parent Application

Path : C:\WINDOWS\explorer.exe

Version : 6.00.2900.2180

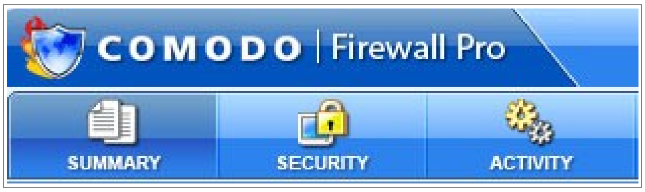
Company : Microsoft Corporation

Security : SAFE

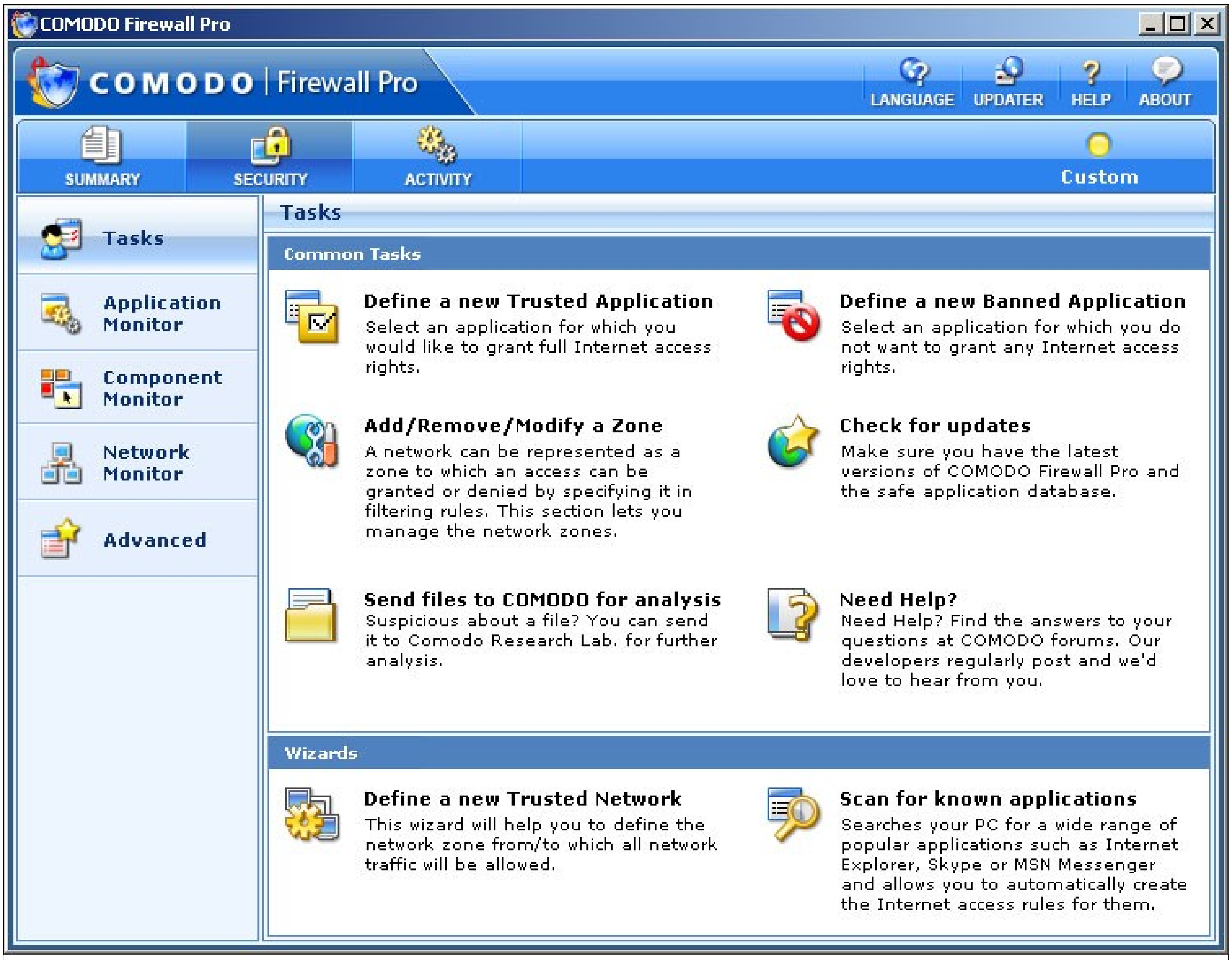
Description : explorer.exe is the Windows Program Manager or Windows Explorer. It manages the Windows Graphical Shell including the Start menu, taskbar, desktop, and File Manager. By removing this process the graphical interface for Windows

Firewall Security

Firewall security is accessed by selecting the 'Security' tab of the main interface:



You can configure the security settings of Comodo Firewall Pro at different levels. The ***Tasks*** feature allows you to create rules for applications and network connections through a series of shortcuts. The ***Application Monitor*** feature allows you to either add/ modify or filter Application filtering rules. The ***Network Monitor*** feature allows you to view configure your network control rules. The ***Advanced*** Configuration allows the user to configure the security settings at an advanced level.



Define a new Trusted Application
Select an application for which you would like to grant full Internet access rights.

Define a new Banned Application
Select an application for which you do not want to grant any Internet access rights.

Add/Remove/Modify a Zone
A network can be represented as a zone to which an access can be granted or denied by specifying it in filtering rules. This section lets you manage the network zones.

Check for updates
Make sure you have the latest versions of COMODO Firewall Pro and the safe application database.

Send files to COMODO for analysis
Suspicious about a file? You can send it to Comodo Research Lab. for further analysis.

Need Help?
Need Help? Find the answers to your questions at COMODO forums. Our developers regularly post and we'd love to hear from you.

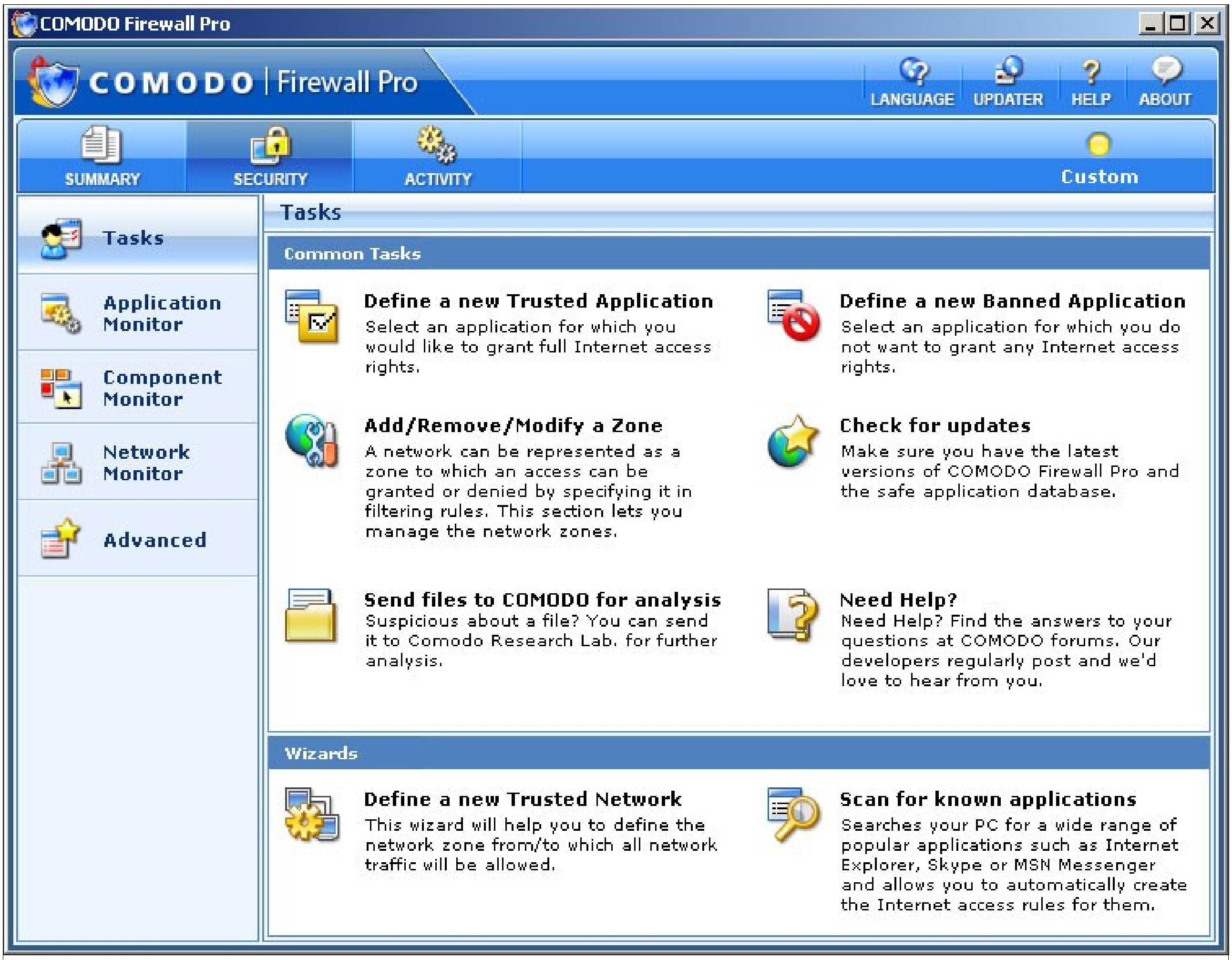
Define a new Trusted Network
This wizard will help you to define the network zone from/to which all network traffic will be allowed.

Scan for known applications
Searches your PC for a wide range of popular applications such as Internet Explorer, Skype or MSN Messenger and allows you to automatically create the Internet access rules for them.

Figure: Firewall Security

Tasks

The ***Tasks*** section allows you to create rules for applications and network connections through a series of shortcuts and wizards. The section contains two main areas, Tasks and Wizards.



Define a new Trusted Application
Select an application for which you would like to grant full Internet access rights.

Define a new Banned Application
Select an application for which you do not want to grant any Internet access rights.

Add/Remove/Modify a Zone
A network can be represented as a zone to which an access can be granted or denied by specifying it in filtering rules. This section lets you manage the network zones.

Check for updates
Make sure you have the latest versions of COMODO Firewall Pro and the safe application database.

Send files to COMODO for analysis
Suspicious about a file? You can send it to Comodo Research Lab. for further analysis.

Need Help?
Need Help? Find the answers to your questions at COMODO forums. Our developers regularly post and we'd love to hear from you.

Define a new Trusted Network
This wizard will help you to define the network zone from/to which all network traffic will be allowed.

Scan for known applications
Searches your PC for a wide range of popular applications such as Internet Explorer, Skype or MSN Messenger and allows you to automatically create the Internet access rules for them.

Figure: Create Rules

Tasks

►**Define a New Trusted Application**

►**Define a New Banned Application**

►**Add / Remove / Modify a Zone**

►**Send files to COMODO for analysis**

►**Need Help**

►**Check for Updates**

Wizards

► **Define a new Trusted Network**

► **Scan For Known Applications**

Define a New Allowed/ Trusted Application

This shortcut represents a convenient way to create an automatic allow rule by configuring the level of "trust" that individual applications have. Comodo Firewall Pro allows you to prepare a list of trusted/ allowed applications and configure their access rights to networks and the internet.

1. Click on **Add a New Allowed / Trusted Application** link.

2. A dialogue box will appear asking you the select the application to be allowed.

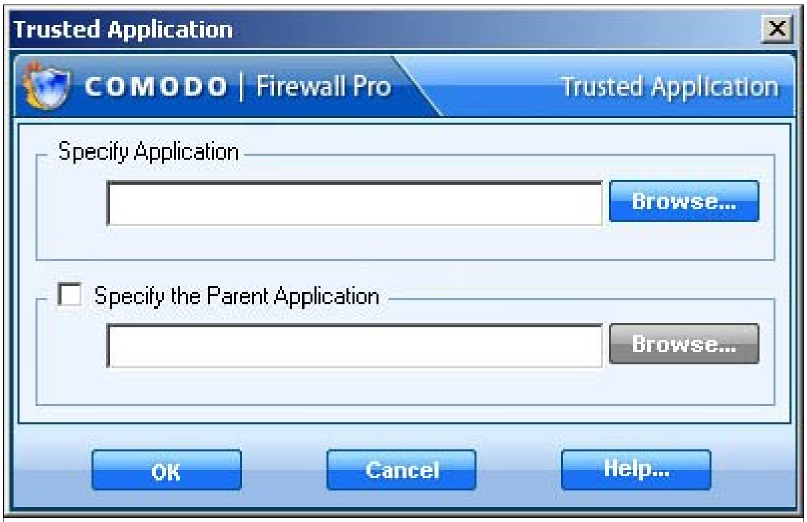
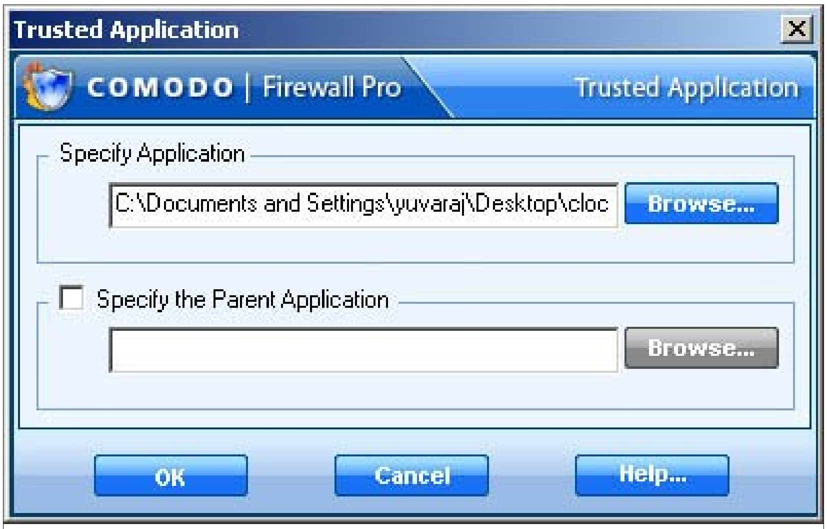


Figure: Select Application to be allowed

3. Click browse to locate the application on your local or network drive.



C:\Documents and Settings\yuvaraj\Desktop\cloc

Figure: Application to be allowed selected

4. The selected application appears along with its location in file system path .

5. You are given the option to specify an application’s parent as well. Check the box and browse to locate the Parent Application. The Firewall will automatically learn it even if it is not specified.

Comodo Firewall Pro verifies the integrity of the application trying to communicate. If this is modified - you are informed. By tracing an application's parent process the firewall knows if another application is trying to spawn an already trusted application and thus deny access to the network even for that trusted application. This system provides the very highest protection against trojans and malware that try to use trusted software such as Internet Explorer to sneakily access the internet.

6. Click OK to finalize the settings. An entry about the Trusted/Allowed Application will appear in the list of Application Control Rules viewable in the Application Monitor section. The Rule takes effect immediately and the application is classified as Trusted/ Allowed so that inbound and outbound connections are permitted. When an application seeks internet access, Comodo Firewall Pro first checks whether it recognizes the application as trusted/ allowed or banned. If the application is recognized as trusted/ allowed, Comodo Firewall Pro automatically allows it access to the Internet.

7. Click Help to view the Help page for how to add a new allowed application.

Define a New Banned Application

If you do not recognize a program then we would recommend that you block it from accessing the internet. If you later identify the application or realize that a program has stopped working because of this action, you can change its settings in the Application Control Rules list.

This shortcut represents a convenient way to create an automatic 'block' rule for an application and to fine-tune its access rights to networks and the internet.

1. Click on **Define a New Banned Application** link in the Tasks section.
2. A dialogue box will appear asking you the select the application to be banned.

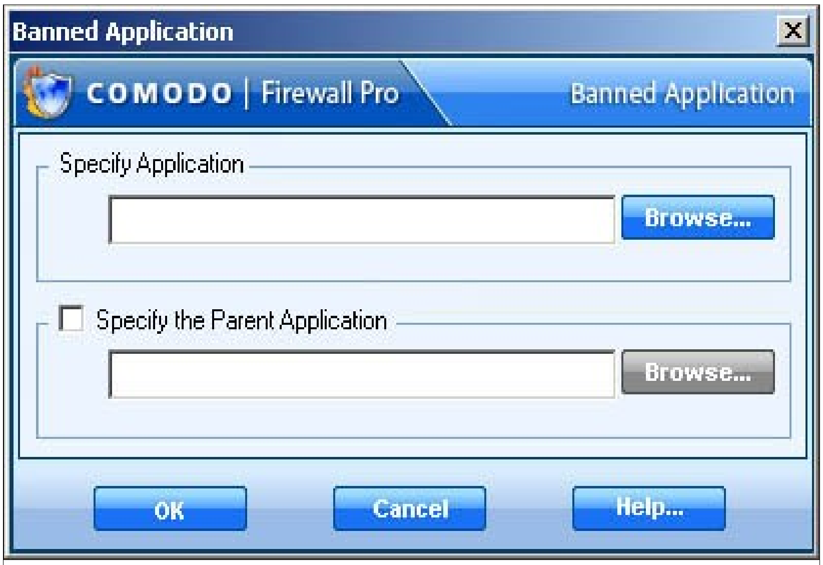
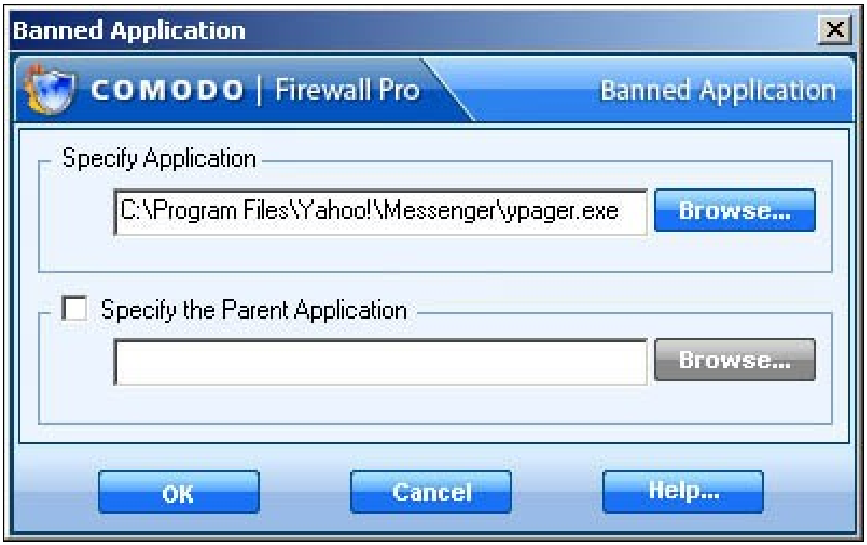


Figure: Select Application to be banned

3. Click 'Browse' to locate the application on your computer.



C:\Program Files\Yahoo!\Messenger\ypager.exe

☐ Specify the Parent Application

Figure: Application to be banned selected

4. The selected application appears along with its location in file system path.
5. You are given the option to specify an application's parent as well. Check the box and browse to locate the Parent Application. The Firewall will automatically learn it even if it is not specified.

Comodo Firewall Pro verifies the integrity of the application trying to communicate. If this is modified - you are informed.

6. Click OK to finalize the settings. An entry about the Banned Application will appear in the list of Application Control Rules. The Rule takes effect immediately and the application is classified as Banned so that inbound and out bound connections are disallowed. When an application seeks Internet access, Comodo Firewall Pro first checks whether it recognizes the application as trusted or banned. If the application is recognized as banned, Comodo Firewall Pro automatically disallows it access to the Internet.

7. If you do not want application to be banned, click cancel.

8. Click Help to view the Help page for how to add a new banned application.

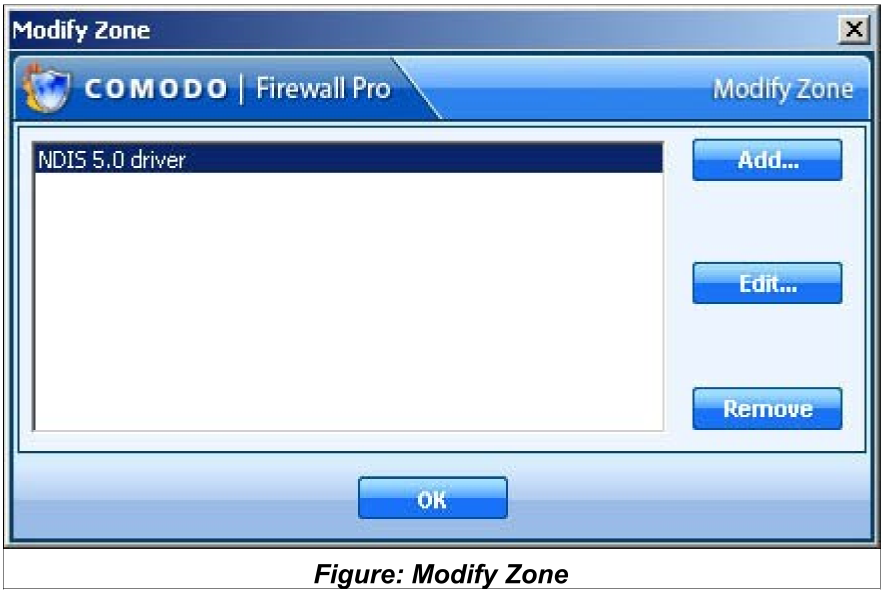
Add/Remove/Modify a Zone

An individual machine or network can be represented as a zone to which access can be granted or denied in Application Control Rules and Network rules. This section lets you Add/Edit/Remove Zones.

Comodo Firewall Pro allows users to add/edit/remove zone through "Modify Zone" dialog box

1. Click on **Add/Remove/Modify a Zone** in the Tasks section.

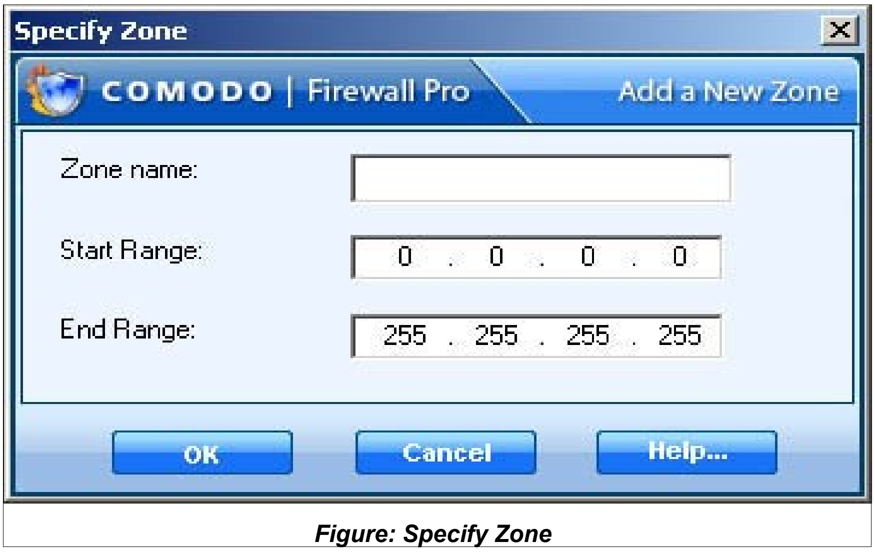
2. A dialogue box will appear asking you to add/edit/remove zone.



NDIS 5.0 driver

Figure: Modify Zone

Click the “Add...” button to define a new zone:



Zone name:

Start Range: 0 . 0 . 0 . 0

End Range: 255 . 255 . 255 . 255

Figure: Specify Zone

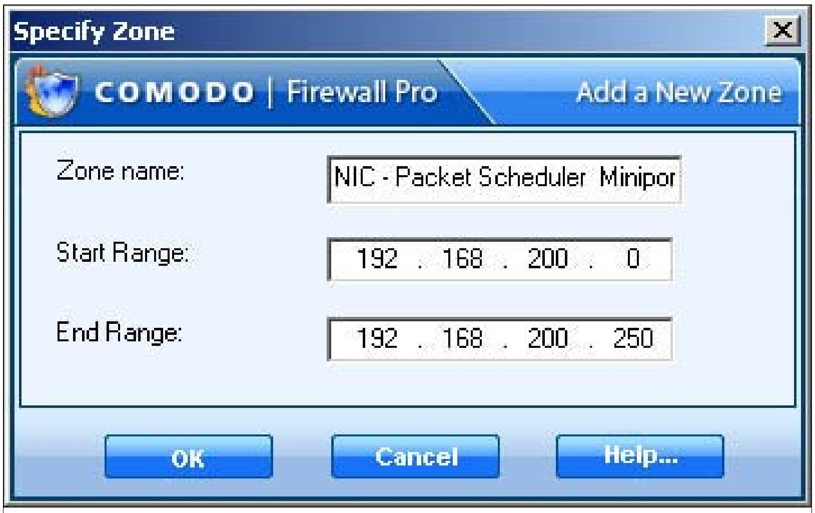
(1) Give the Zone a name , for example ‘Home'

(2) Enter the IP for the zone, starting from the Start IP to the End IP range for which you want unrestricted access. The addresses you define here specify the IP(s) that traffic can be directed to from the Internet.

(3) Click OK to create the new Zone rule.

(4) Repeat for any other zones which you want to add.

If you want to edit any zone for Name/Start IP/ End IP, You can select it from the list and click on "Edit..." button and again just like "Add" you can modify each field of it.



Zone name: NIC - Packet Scheduler Minipor

Start Range: 192 . 168 . 200 . 0

End Range: 192 . 168 . 200 . 250

Figure: Edit Zone

In case you want to remove a particular zone, you can select it from the list and click on “Remove” button.

Send files to Comodo for analysis

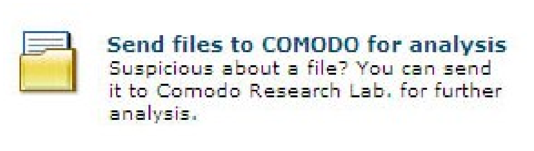
If there is no advice available for an application and/or parent and they are not in the Comodo Firewall Pro safe list, then you have the option to submit them to Comodo for analysis. Clicking the "Send files to COMODO for analysis" link will automatically begin the file submission process.

After sending the file to us, our developers will determine whether or not it represents a threat to your security. If it does we will take immediate action to nullify it.

The submit function is an important component of our coordinated strategy to combat emerging threats to your security.

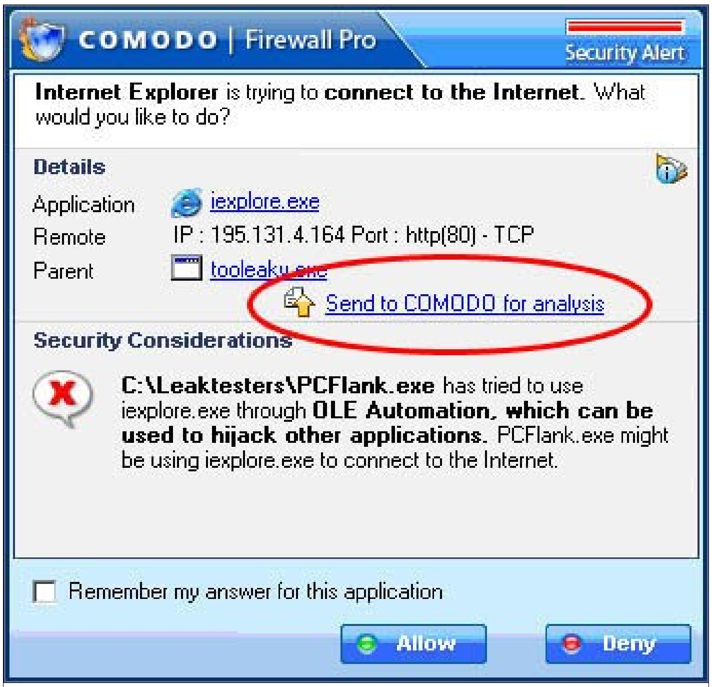
Users can access the submit feature in two ways.

The first is by clicking on 'Send files to COMODO for analysis in the main Common Tasks interface (shown below)



Send files to COMODO for analysis
Suspicious about a file? You can send it to Comodo Research Lab. for further analysis.

Secondly, users can send a file to us as soon as Comodo Firewall Pro detects straight from an alert that is generated. (see below). Simply click the link to go straight to the files submission process.



Internet Explorer is trying to **connect to the Internet**. What would you like to do?

Details

Application iexplore.exe

Remote IP : 195.131.4.164 Port : http(80) - TCP

Parent tooleaky.exe

Send to COMODO for analysis

Security Considerations

C:\Leaktesters\PCFlank.exe has tried to use iexplore.exe through **OLE Automation, which can be used to hijack other applications.** PCFlank.exe might be using iexplore.exe to connect to the Internet.

□ Remember my answer for this application

Figure: Instant submission via the alert

File Submission Process

Comodo Firewall Pro allows users to send files for analysis which are not in the safe list through "Files Submission" dialog box as below.

1. Click on "Send files to COMODO for analysis"

2. The 'Files Submission' dialog allows you to choose which files you wish to submit. Click 'Add' to manually add suspicious files to the 'List of Files'. Similarly, to remove a file from the submission process, click the 'Remove' button. You have the option to add an accompanying description to each file you submit.

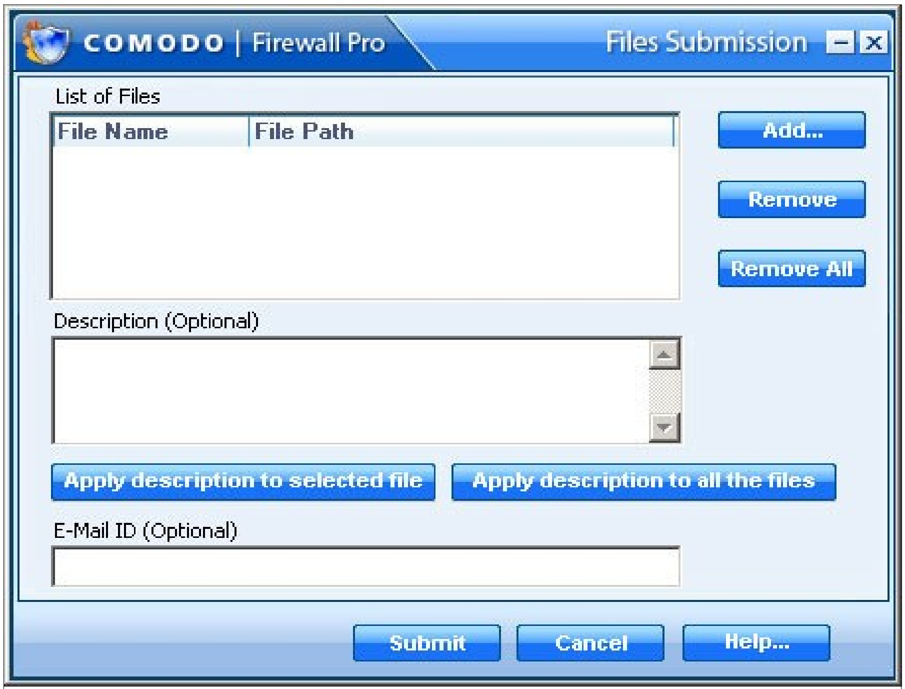
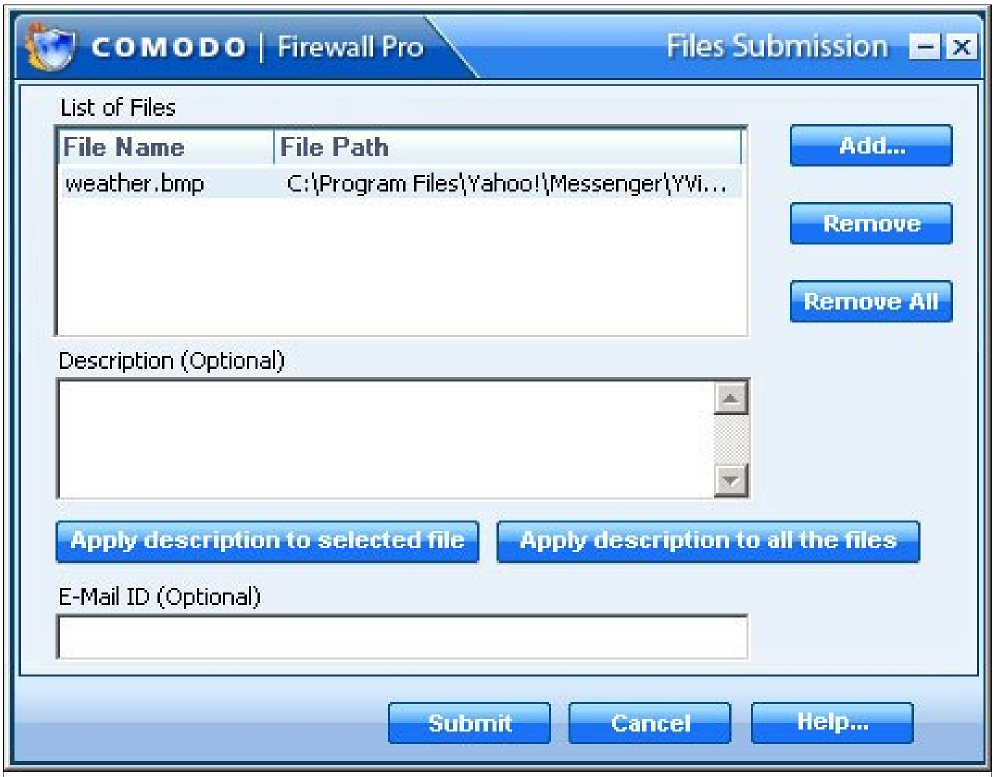


Figure: Send files to COMODO

Using “Add...” button you can add a file, which will bring up following dialog:



File Name	File Path
weather.bmp	C:\Program Files\Yahoo!\Messenger\YVi...

Figure: Send files to COMODO - Add

In case you want to remove a particular file, you can select it from the list and click on “Remove” button and if you want to remove all the files in the list Click on "Remove All" button.

Click 'Submit' to send the files to Comodo.

Need Help?

Comodo Forums

The fastest way to get further assistance on Comodo Firewall Pro is by joining Comodo Forums, a message board exclusively created for our users to discuss anything related to our products. Register free at http://forums.comodo.com .

You’ll benefit from the expert contributions of developers and fellow users alike and we'd love to hear your thoughts and suggestions.

Users can also access the forums by clicking "Need Help?" in the 'Tasks' main screen.

Online Knowledge Base

We also have an online knowledge base and support ticketing system at http://support.comodo.com . Registration is free.

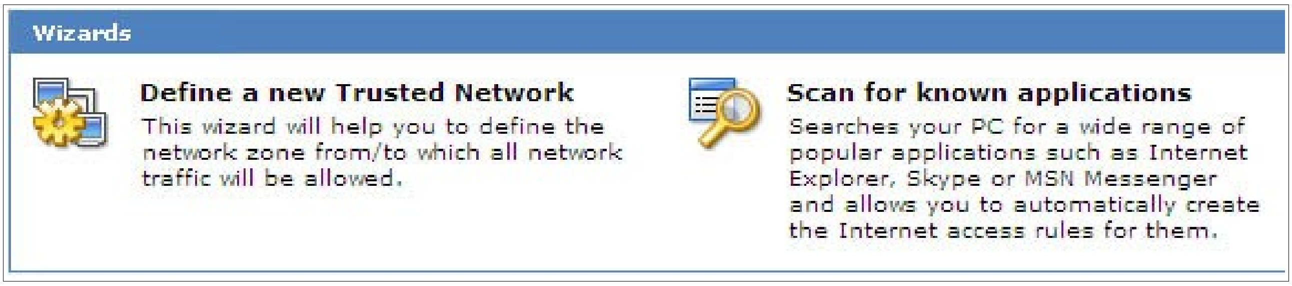
Check for Updates?

To download the updates manually,Click on the Updater icon at the top right hand corner of the application:

To know more see Manual Updater and Automatic Updater.

Wizards

If you use specific services that require Internet or network access on a regular basis, you may want to adjust access settings for these services or machines. You can configure security settings for each application on your computer by setting certain restrictions on which IP addresses and ports an application can utilize.



Wizards

Define a new Trusted Network
This wizard will help you to define the network zone from/to which all network traffic will be allowed.

Scan for known applications
Searches your PC for a wide range of popular applications such as Internet Explorer, Skype or MSN Messenger and allows you to automatically create the Internet access rules for them.

Comodo Firewall Pro can scan your computer for applications which seek Internet-access and create access rules for them. When the scan is complete, you can use the results to determine which programs should have access to the Internet and, if desired, adjust their access rules. Comodo Firewall Pro has the following wizards:

► **Define a new Trusted Application**

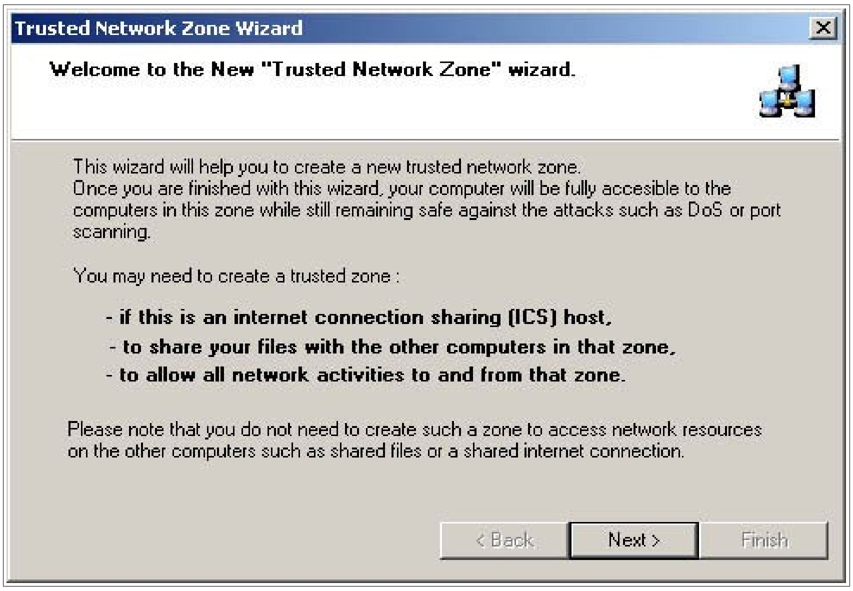
► **Scan For Known Applications**

Define a new Trusted Network

The Trusted Network Zone Wizard

Computers or Web sites in the Trusted Zone have full access to your computer. The trusted zone is for machines you trust - filesharing is allowed, and by default no stealthing is done. The Trusted zone includes the computer under protection and usually the local network and allows any network operations. These network operations are expected safe because the zone is trusted. There are still some restrictions though, to prevent fragmented packets or denial of service type attacks and port scanning.

You can specify the addresses of trusted machines and websites either by name or by IP address.



Trusted Network Zone Wizard

Welcome to the New "Trusted Network Zone" wizard.

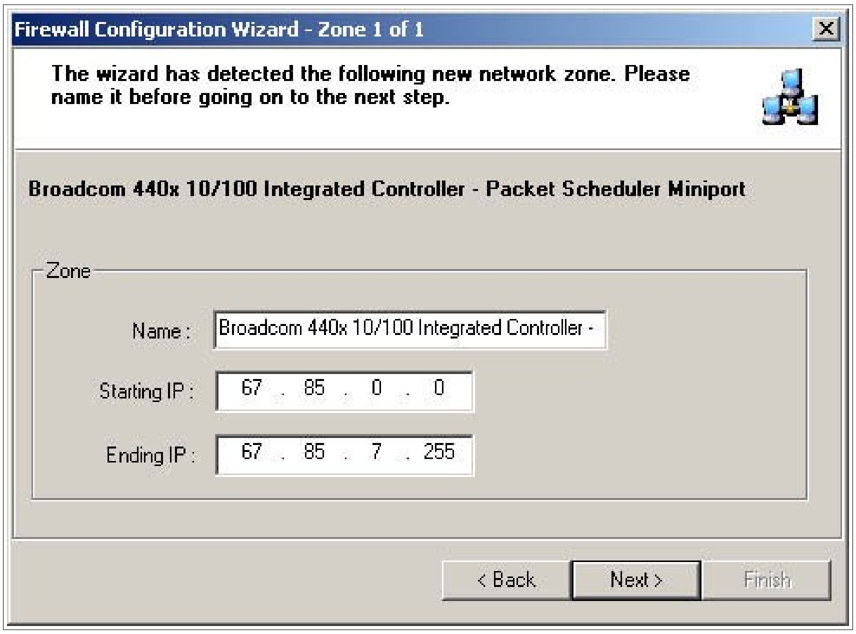
This wizard will help you to create a new trusted network zone.
Once you are finished with this wizard, your computer will be fully accesible to the computers in this zone while still remaining safe against the attacks such as DoS or port scanning.

You may need to create a trusted zone :

- **if this is an internet connection sharing (ICS) host,**
- **to share your files with the other computers in that zone,**
- **to allow all network activities to and from that zone.**

Please note that you do not need to create such a zone to access network resources on the other computers such as shared files or a shared internet connection.

To begin adding a trusted zone, click 'Next'.



Firewall Configuration Wizard - Zone 1 of 1

The wizard has detected the following new network zone. Please name it before going on to the next step.

Broadcom 440x 10/100 Integrated Controller - Packet Scheduler Miniport

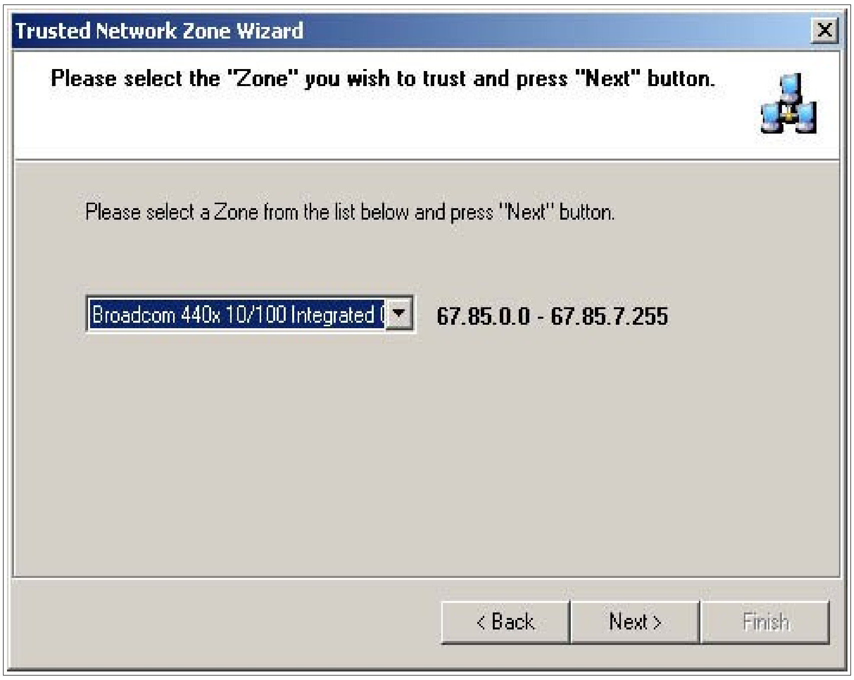
Zone

Name : Broadcom 440x 10/100 Integrated Controller -

Starting IP : 67 . 85 . 0 . 0

Ending IP : 67 . 85 . 7 . 255

The wizard auto-detects any new network zones and displays the range of IP addresses to be contained within the trusted zone. This will usually represent your computer and other machines on your local network. Click next to continue:



Trusted Network Zone Wizard

Please select the "Zone" you wish to trust and press "Next" button.

Please select a Zone from the list below and press "Next" button.

Broadcom 440x 10/100 Integrated (67.85.0.0 - 67.85.7.255

You are now required to selected the network zone you wish to 'Trust'. Select the network zone from the drop down list and click 'Next'. At the ensuing confirmation dialog, please take a moment to review your settings and click 'Finish'. If you wish to alter settings at any time, press 'Back'.

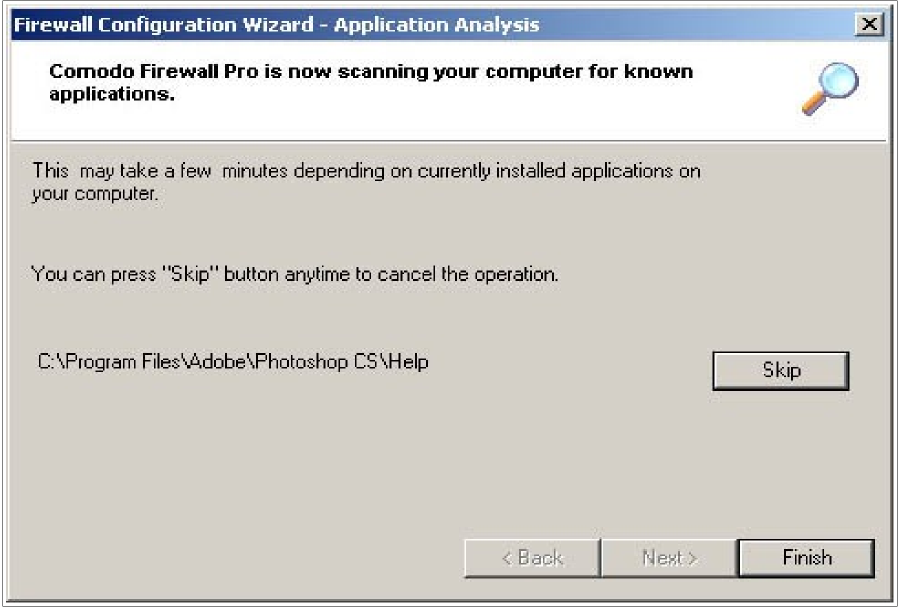
Scan for Known Applications

The Scan for Known Applications Wizard

The 'Scan for Known Applications' wizard is used to create automatic rules for a wide range of popular applications, including Internet Explorer, Skype, FireFox, MSN Messenger. It also creates automatic rules for critical system processes such as svchost.exe.

Using the 'Scan for known applications' wizard instructs Comodo Firewall Pro to audit the applications currently installed on your computer.

The wizard will search your system for applications it recognizes and will then ask you if you want to grant the permissions it needs to operate.



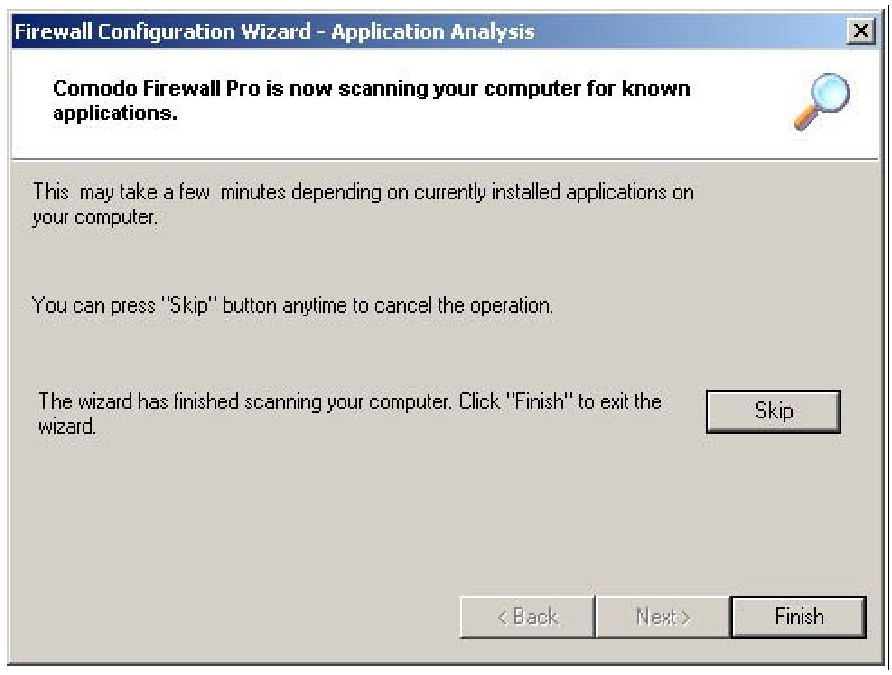
Firewall Configuration Wizard - Application Analysis

Comodo Firewall Pro is now scanning your computer for known applications.

This may take a few minutes depending on currently installed applications on your computer.

You can press "Skip" button anytime to cancel the operation.

C:\Program Files\Adobe\Photoshop CS\Help



Firewall Configuration Wizard - Application Analysis

Comodo Firewall Pro is now scanning your computer for known applications.

This may take a few minutes depending on currently installed applications on your computer.

You can press "Skip" button anytime to cancel the operation.

The wizard has finished scanning your computer. Click "Finish" to exit the wizard.

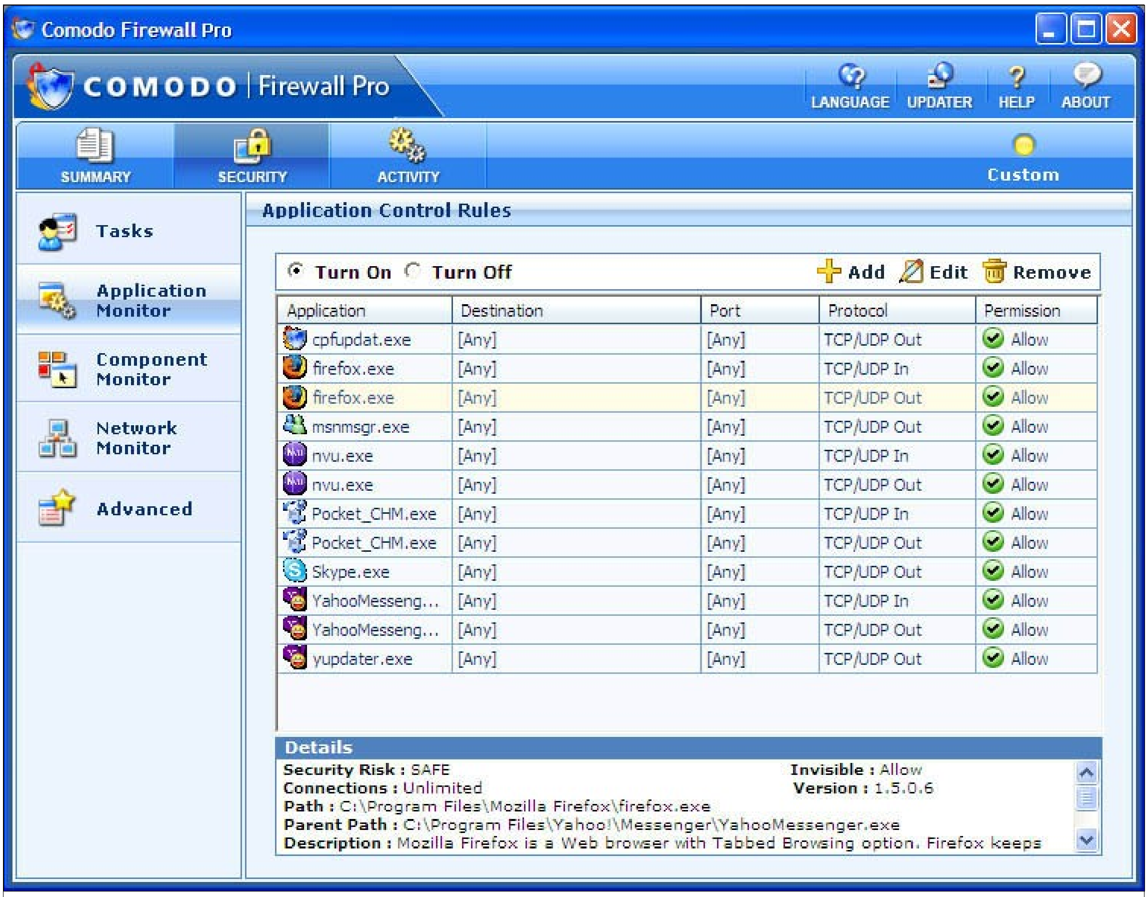
Application Monitor

Using Comodo Firewall Pro, you can protect your system, beginning with the individual applications that you have running on your system. Using Application Control rules, you can set the permission status of an application.

Application filtering rules can be added/modified/deleted through Application Control Rule attributes.

Application Control Rules

Click on the 'Security tab' then the *Application Monitor* tab in the main firewall interface. The interface will then display a list of applications alongside various, user configurable attributes.



● Turn On ○ Turn Off

Application	Destination	Port	Protocol	Permission
cpfupdat.exe	[Any]	[Any]	TCP/UDP Out	✓ Allow
firefox.exe	[Any]	[Any]	TCP/UDP In	✓ Allow
firefox.exe	[Any]	[Any]	TCP/UDP Out	✓ Allow
msnmsgr.exe	[Any]	[Any]	TCP/UDP Out	✓ Allow
nvu.exe	[Any]	[Any]	TCP/UDP In	✓ Allow
nvu.exe	[Any]	[Any]	TCP/UDP Out	✓ Allow
Pocket_CHM.exe	[Any]	[Any]	TCP/UDP In	✓ Allow
Pocket_CHM.exe	[Any]	[Any]	TCP/UDP Out	✓ Allow
Skype.exe	[Any]	[Any]	TCP/UDP Out	✓ Allow
YahooMesseng...	[Any]	[Any]	TCP/UDP In	✓ Allow
YahooMesseng...	[Any]	[Any]	TCP/UDP Out	✓ Allow
yupdater.exe	[Any]	[Any]	TCP/UDP Out	✓ Allow

Details

Security Risk : SAFE **Invisible :** Allow
Connections : Unlimited **Version :** 1.5.0.6
Path : C:\Program Files\Mozilla Firefox\firefox.exe
Parent Path : C:\Program Files\Yahoo!\Messenger\YahooMessenger.exe
Description : Mozilla Firefox is a Web browser with Tabbed Browsing option. Firefox keeps

Figure: Application Control Rules

Column Description

1. The First Column ***(Application)*** represents each application's icon and name (description) — if the application has no icon, the default system icon for executable files will be used; if no description (name) is available, the name of the file without the extension will be displayed.
2. The Second Column ***(Destination)*** represents the remote IP Address of the application.
3. The Third Column ***(Port)*** represents the Port Numbers of individual applications.
4. The Fourth Column ***(Protocol)*** represents the Protocol, usually TCP, UDP or Both, as well as direction of communication as Incoming or Outgoing.

5. The Fifth Column ***(Permission)*** represents the action taken by the firewall like Allowed , Trusted , Disallowed etc..

Selecting any of the applications in the first column also displays addition information in the 'Details' panel at the foot of the screen. These are:

Secutity Risk - the file path of individual applications.

Connections - the state of connection of the application as established at the rate of number per minute.

Path - the file path of individual application on your hard drive.

Parent path - the Parent application's location on your hard drive.

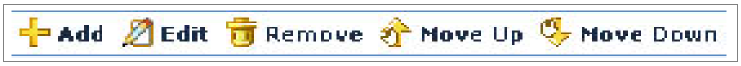
Description - The name of the application. If the application is in the firewall database, you will see a brief outline of the production functionality and main features.

Invisible- Which action the firewall should take if this application attempts to make an invisible connection. This feature is set in the Application Rules/Miscellaneous tab.

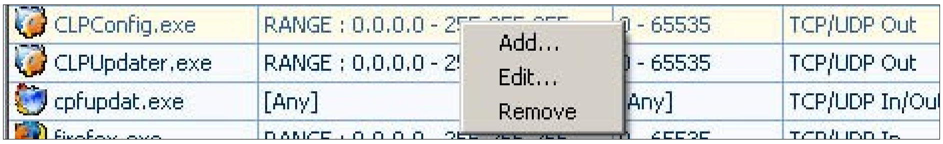
Version- The specific version number of the application you have selected.

Add / Edit an Application Control Rule

You can add or modify or remove an application control rule by clicking on the **Add/ Edit/ Remove** buttons at the top of the list:



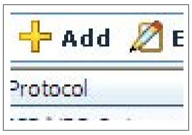
Alternatively, selecting any application and right clicking will display a context sensitive menu of the same functionality:



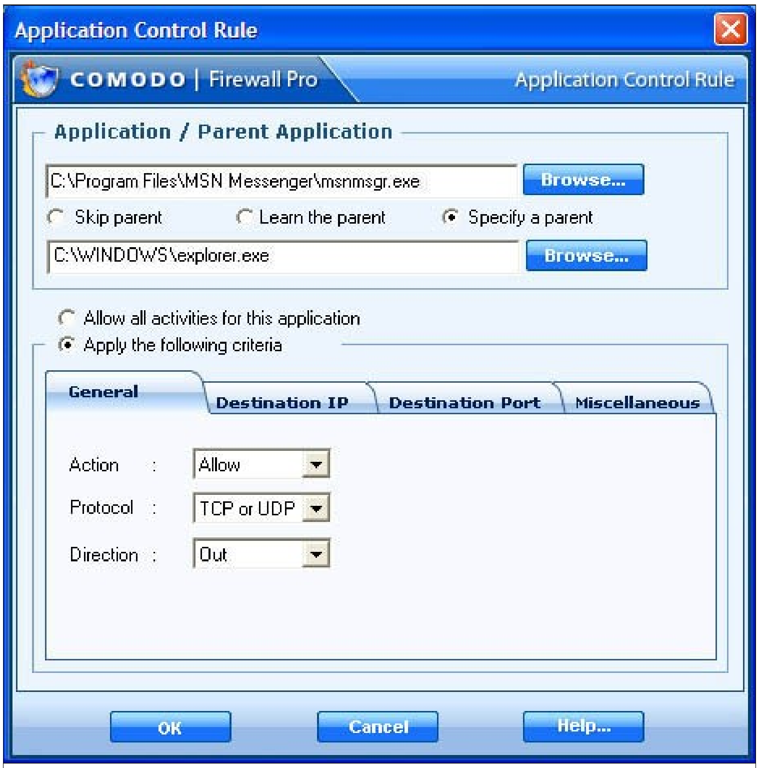
CLPConfig.exe	RANGE : 0.0.0.0 - 255.255.255	0 - 65535	TCP/UDP Out
CLPUpdater.exe	RANGE : 0.0.0.0 - 2	0 - 65535	TCP/UDP Out
cpfupdat.exe	[Any]	Any]	TCP/UDP In/Out
firefox.exe	RANGE : 0.0.0.0 - 255.255.255	65535	TCP/UDP In

Add a New Application Control Rule

To create a new application control rule, click the 'Add' button at the top right corner of Application Monitor.



A dialogue box will appear allowing you to configure the new application rule:



Application Control Rule

COMODO | Firewall Pro — Application Control Rule

Application / Parent Application

C:\Program Files\MSN Messenger\msnmsgr.exe — Browse...

○ Skip parent ○ Learn the parent ● Specify a parent

C:\WINDOWS\explorer.exe — Browse...

○ Allow all activities for this application

● Apply the following criteria

General | Destination IP | Destination Port | Miscellaneous

Action : Allow

Protocol : TCP or UDP

Direction : Out

Figure: Add Application Rule

Select the Application

1. Click 'Browse' to locate the new application on your computer's hard drive. In this case we have chosen MSN Messenger.
2. The selected application appears along with its location in file system path.
3. You are given the option to specify an application’s parent as well. Check the appropriate radio button to browse to the Parent Application. The Firewall will automatically learn it even if it is not specified.

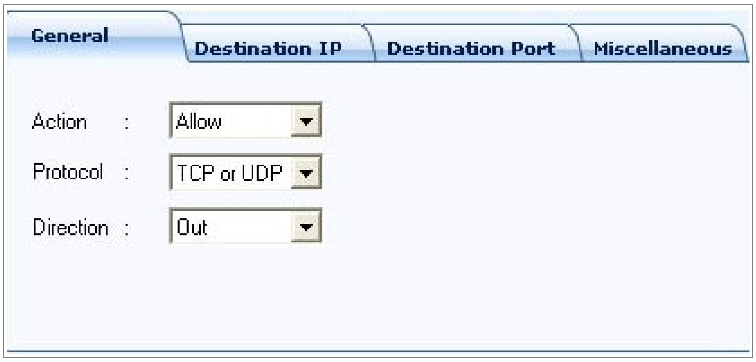
Comodo Firewall Pro verifies the integrity of the application trying to communicate. If this is modified - you are informed. By tracing an application's parent process the firewall knows if another application is trying to spawn an already trusted application and thus deny access to the network even for that trusted application.

HELP

Click ***Help*** to view the Help page for how to add a new application control rule.

If you want specify the network to be allowed access you will have to provide details about Host IP Address, Services Port and select the mode of Action, Direction & Protocol. This is done using the four tabs at the foot of the Application Control Window.

'General' tab



General | Destination IP | Destination Port | Miscellaneous

Action : Allow

Protocol : TCP or UDP

Direction : Out

This area allows you to specify general attibutes concerning an applications rule. From here you can instruct the Firewall on whether to allow an application to connect, using which protocol and in which direction information is permitted to move.

Action

Select the action you want Comodo Firewall Pro to take when the rule is matched. Select from **Allow, Deny** or **Ask** as the action you wish the Firewall to take.

Protocol

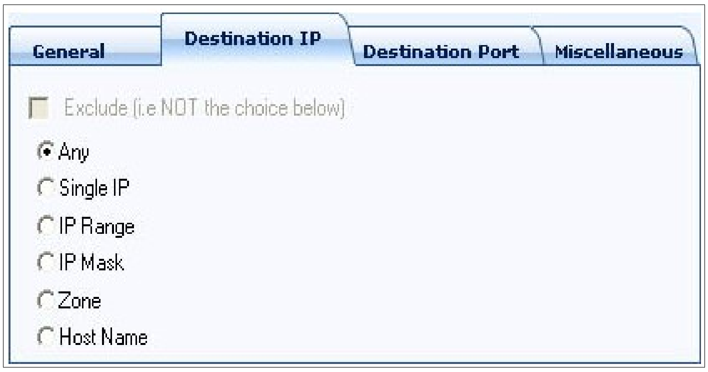
All information sent over the Internet is communicated using a protocol called TCP/IP. Because all of the computers on the Internet understand this protocol, each one can communicate with every other computer on the Internet. TCP and IP are separate parts of this protocol.

Now you should select the protocol as TCP (**Transmission Control Protocol**), UDP (**User Datagram Protocol**), or Both (TCP/ UDP) used by the application(s).TCP is the standard for file transfers, as it has built-in error handling. UDP is faster than TCP, but doesn't provide error handling. It's normally used for streaming data, such as video feeds and on-line games, where loss of data is of less importance.

Direction

Then select the direction of connection whether it is made by a remote computer (**In**), by you (**Out**), or if it has been established by **Both**.

'Destination IP' tab



□ Exclude (i.e NOT the choice below)

● Any
○ Single IP
○ IP Range
○ IP Mask
○ Zone
○ Host Name

When you're connected to a network, for example the Internet, your computer, as any other computer, is assigned a unique identification. This is called an ***IP address***. It consists of 4 groups of numbers, ranging from 0 to 255, separated by a dot.

Example: 192.168.200.113

Specify the hosts IP addresses from which you will allow or deny connections. You can select the IP Addresses number(s) from the list.

Select the IP address:

1. You can choose any IP Address by selecting Any .This menu defaults to the IP range of 0.0.0.0- 255.255.255.255 to allow connection from all IP addresses.

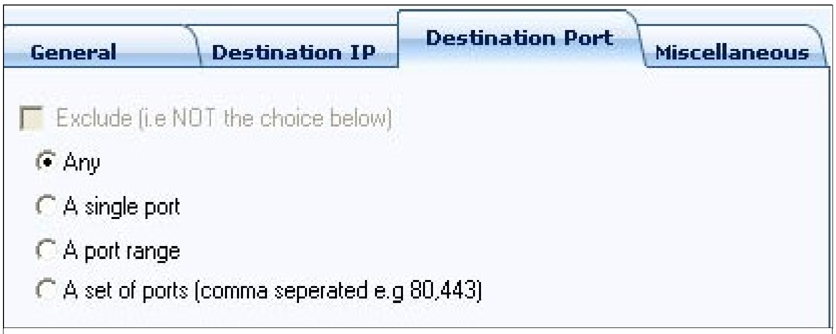
2. You can choose a Single IP address by selecting Single and entering the IP address in the IP address text box, for ex, 192.168.200.113.

3. You can choose an IP Range by selecting IP Range for example the range in your private network and entering the IP addresses in the Start Range and End Range text boxes.

4. You can choose IP address / mask by selecting IP Mask. 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.
5. You can choose an entire zone by selecting Zone .This menu defaults to the zone first defined during installation. But you can also define your own zone by first creating a Zone through the Add a Zone shortcut.
6. You can choose to give a name by selecting Host Name which denotes your IP address.

Exclude (i.e. NOT the choice below)

The opposite of what you specify is applicable.
So if you Check the Exclude box in, say, the 'Destination IP' tab and enter values for the IP range, those values will be not be applicable and values other than those specified become applicable. If you have chosen to exclude a certain range of IP addresses, you will have to create a seperate 'Application Rule' for the range of IP addresses that you DO want to use.
The exclude feature is limited to the subject tab and does not affect any other parameters you choose within the specific rule - so you can have one Application rule that 'Excludes' certain IP addresses whilst 'Including' certain Ports.
'Destination Port' tab

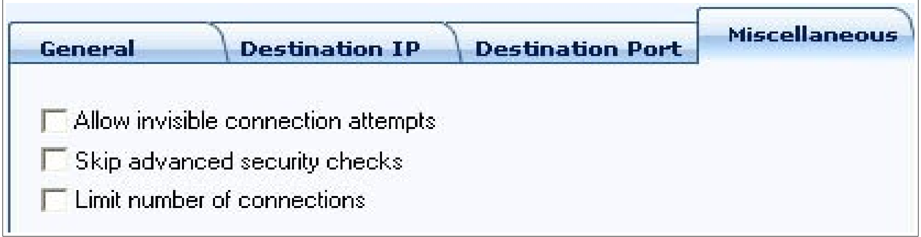


□ Exclude (i.e NOT the choice below)
● Any
○ A single port
○ A port range
○ A set of ports (comma seperated e.g 80,443)

Figure: Define Port

A Port Number is used to decide which service you are about to use, for example , Web browsing HTTP has a port number of 80.
You must enter which ports are used by the application(s), by selecting the port number(s) from the list.
Define Port Types:
1. You can choose any port number by selecting Any - set by default , 0- 65535.
2. You can choose a Single Port number by selecting Single Port and selecting the single port numbers from the list.
3. You can choose a Port Range by selecting Port Range and selecting the port numbers from the From and To list.
4. You can choose a set of ports seperated by commas eg 80;443)

'Miscellaneous' tab



□ Allow invisible connection attempts
□ Skip advanced security checks
□ Limit number of connections

Allow invisible connection attempts
Checking this box means the application is trusted to make invisible connections to the internet and will not generate an alert.

Skip advanced security checks

This option is for applications which user allows but still for some reasons they fail to connect. eg. AVG e-mail scanner.

Limit number of connections

This controls the amount of connections per minute that an application can create. If you select this feature, then the menu defaults to a limit of 10 connections per minute.

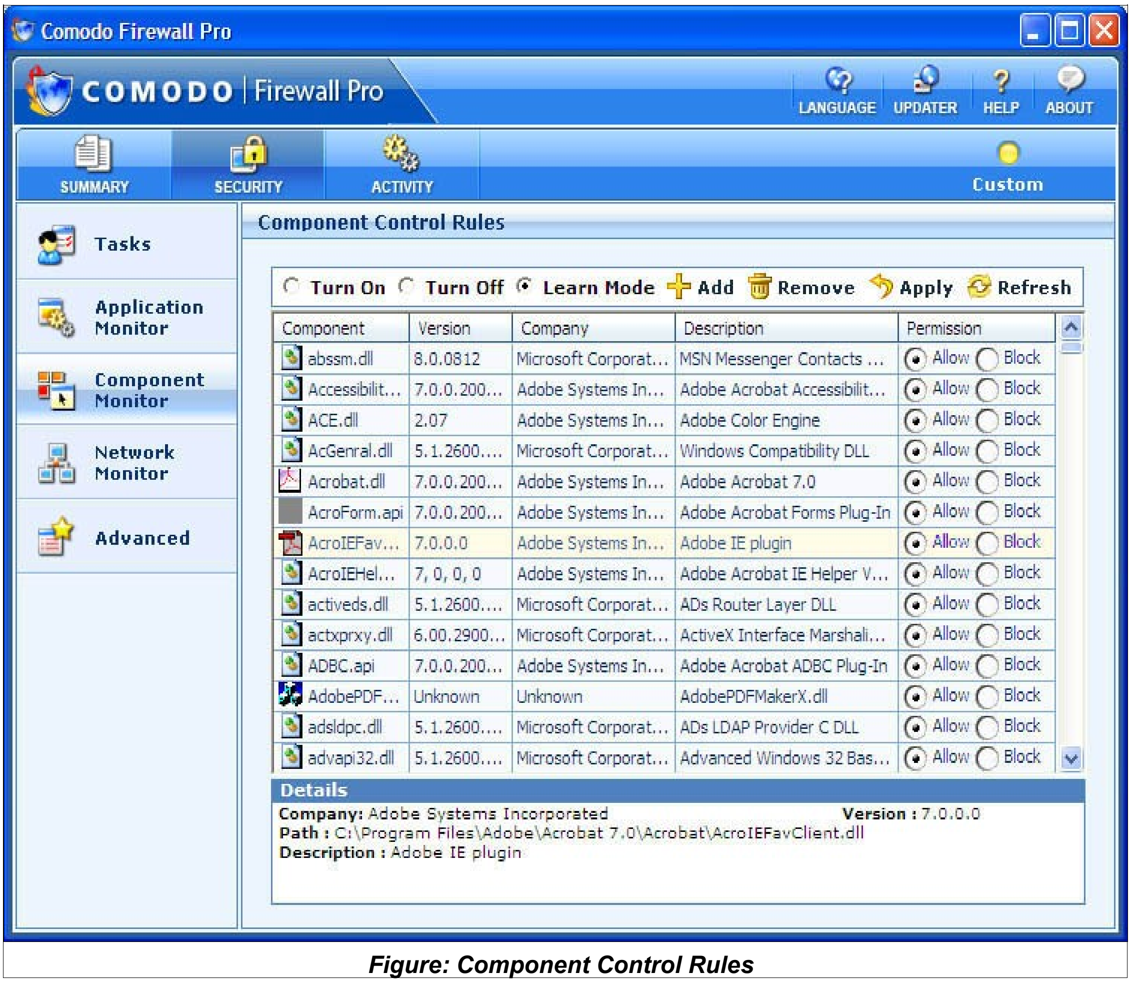
Component Monitor

A component, when loaded into application's memory, acts as a part of that application hence having the same network access rights as the application itself.

Comodo Firewall Pro now validates all the components of an application before granting the Internet access. These components may be dynamic link libraries or ActiveX components that an application is using.
Component Control Rules can be added, removed and applied via the Component Monitor.

Component Control Rules

Click on the 'Security tab' then the *Component Monitor* button. The interface will then display a list of
Components alongside various user configurable attributes.



Component	Version	Company	Description	Permission
abssm.dll	8.0.0812	Microsoft Corporat...	MSN Messenger Contacts ...	● Allow ○ Block
Accessibilit...	7.0.0.200...	Adobe Systems In...	Adobe Acrobat Accessibilit...	● Allow ○ Block
ACE.dll	2.07	Adobe Systems In...	Adobe Color Engine	● Allow ○ Block
AcGenral.dll	5.1.2600....	Microsoft Corporat...	Windows Compatibility DLL	● Allow ○ Block
Acrobat.dll	7.0.0.200...	Adobe Systems In...	Adobe Acrobat 7.0	● Allow ○ Block
AcroForm.api	7.0.0.200...	Adobe Systems In...	Adobe Acrobat Forms Plug-In	● Allow ○ Block
AcroIEFav...	7.0.0.0	Adobe Systems In...	Adobe IE plugin	● Allow ○ Block
AcroIEHel...	7, 0, 0, 0	Adobe Systems In...	Adobe Acrobat IE Helper V...	● Allow ○ Block
activeds.dll	5.1.2600....	Microsoft Corporat...	ADs Router Layer DLL	● Allow ○ Block
actxprxy.dll	6.00.2900...	Microsoft Corporat...	ActiveX Interface Marshali...	● Allow ○ Block
ADBC.api	7.0.0.200...	Adobe Systems In...	Adobe Acrobat ADBC Plug-In	● Allow ○ Block
AdobePDF...	Unknown	Unknown	AdobePDFMakerX.dll	● Allow ○ Block
adsldpc.dll	5.1.2600....	Microsoft Corporat...	ADs LDAP Provider C DLL	● Allow ○ Block
advapi32.dll	5.1.2600....	Microsoft Corporat...	Advanced Windows 32 Bas...	● Allow ○ Block

Details

Company: Adobe Systems Incorporated **Version :** 7.0.0.0
Path : C:\Program Files\Adobe\Acrobat 7.0\Acrobat\AcroIEFavClient.dll
Description : Adobe IE plugin

Figure: Component Control Rules

Column Description

1.The First Column ***(Component)*** represents the component files

2.The Second Column ***(Version)*** represents the version of the components.

3.The Third Column ***(Company)*** represents the developer of the components.

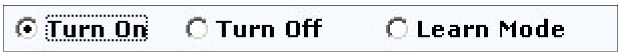
4.The Fourth Column ***(Description)*** represents the description of the components.

5.The Fifth Column ***(Permission)*** represents the action to be taken by the firewall, whether to Allow or Block access. Allow or Block are the two types of permissions:

> 1.**Allow** means allow the internet access request of the application which has the component loaded into its memory.
>
> 2.**Block** means block the application's internet access request while it has the component loaded into its memory.Permissions of a component affect the whole application i.e. according to selected components existence, the whole application will be blocked or allowed access.

Selecting any of the component in the first column also displays additional information in the 'Details' panel at the foot of the screen, where complete path of the component can be seen.

Turn On /Turn Off / Learn Mode on Component Control Rule



● Turn On ○ Turn Off ○ Learn Mode

You can activate/ deactivate Component Monitor by clicking Turn On/ Turn off buttons at the top of the list.

Component monitor 'On'

When Turn On is selected, the Component Monitor section of the Summary screen will dispay

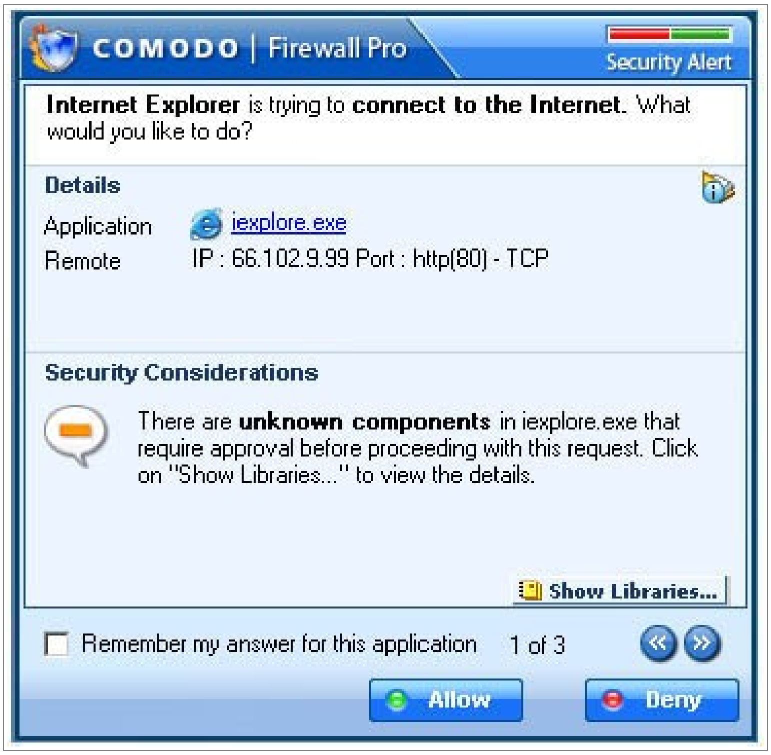
✓ Component Monitor

Figure: Green

This mode forces the firewall to check for the applications' components in memory before granting them internet access.

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. If the firewall detects unknown components (those not listed in the firewall database) then the alert will contain a "Show Libraries..." button. Click to review the components and decide whether or not to grant them access.

An alert similar to the following will appear when one or more components are found which are not listed.



COMODO | Firewall Pro — Security Alert

Internet Explorer is trying to **connect to the Internet**. What would you like to do?

Details

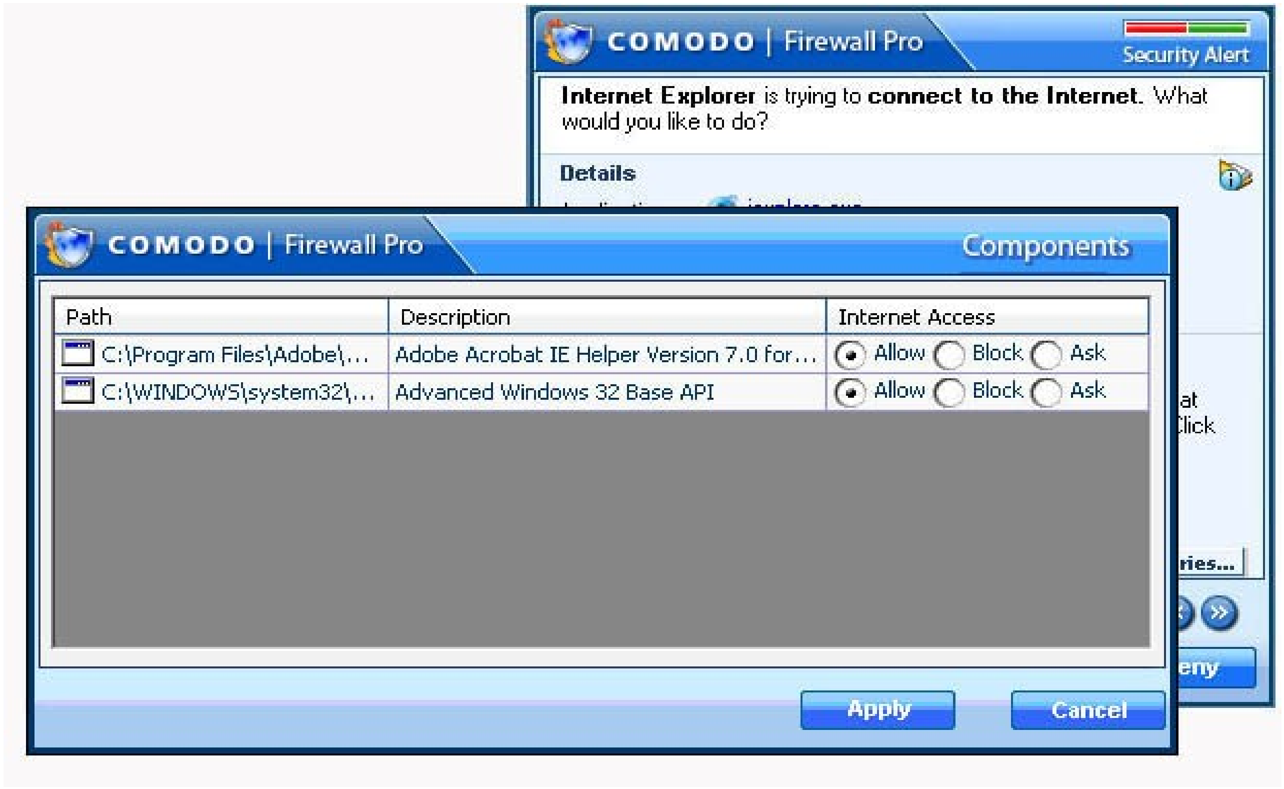
Application iexplore.exe

Remote IP : 66.102.9.99 Port : http(80) - TCP

Security Considerations

There are **unknown components** in iexplore.exe that require approval before proceeding with this request. Click on "Show Libraries..." to view the details.

To check the components click **Show Libraries,** which will show list of components.



COMODO | Firewall Pro — Components

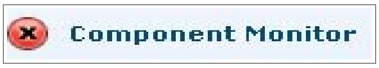
Path	Description	Internet Access
C:\Program Files\Adobe\...	Adobe Acrobat IE Helper Version 7.0 for...	● Allow ○ Block ○ Ask
C:\WINDOWS\system32\...	Advanced Windows 32 Base API	● Allow ○ Block ○ Ask

If any of the components loaded by application is set to be blocked, the application is not allowed to connect. So in order for an application to connect out, all it's components must be allowed.

When you select ***Ask*** against a component, you will be prompted to ***Allow/ Deny*** access every time this component appears in any application's memory

Component monitor 'Off'

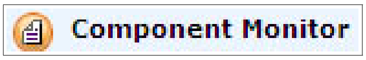
When ***Turn Off*** is selected, the Component Monitor section of the Summary screen will dispay



Deactivating the component monitor means the firewall does not check components loaded by an application making a connection and therefore any rules set for it's components are ignored.

Component monitor 'Learn Mode'

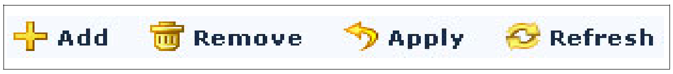
When you install Comodo Firewall the Component Montitor is set to 'Learn' mode by default



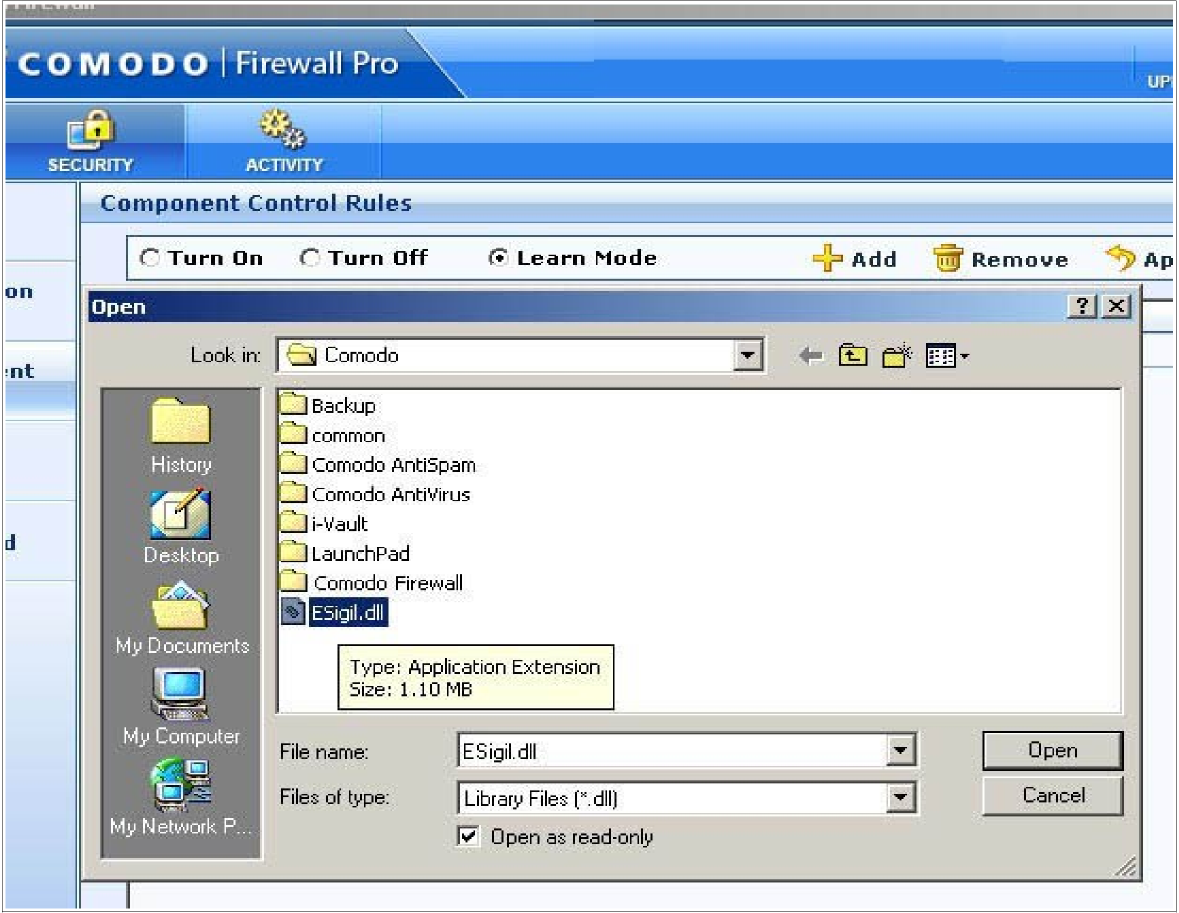
Whereas the number of internet accessing applications will usually be relatively small, there is always a huge number of components loaded within these applications. By enabling learn mode the firewall will be forced to learn and build the component profile of the PC. Whenever an allowed application attempts to connect to the internet, Comodo Firewall will add all the components it loads to the control rule list. By default, each of these components inherit the applications 'Allow' status. Users have the option to change this status by selecting one the appropriate Allow/Block/Ask radio button.

Add / Remove an Component Control Rule

You can add or remove an Component control rule by clicking on the Add/ Remove buttons at the top of the list:



Add: Opens a new component dialog and lets you chose the component you want to add as a rule.



Look in: Comodo

Type: Application Extension
Size: 1.10 MB

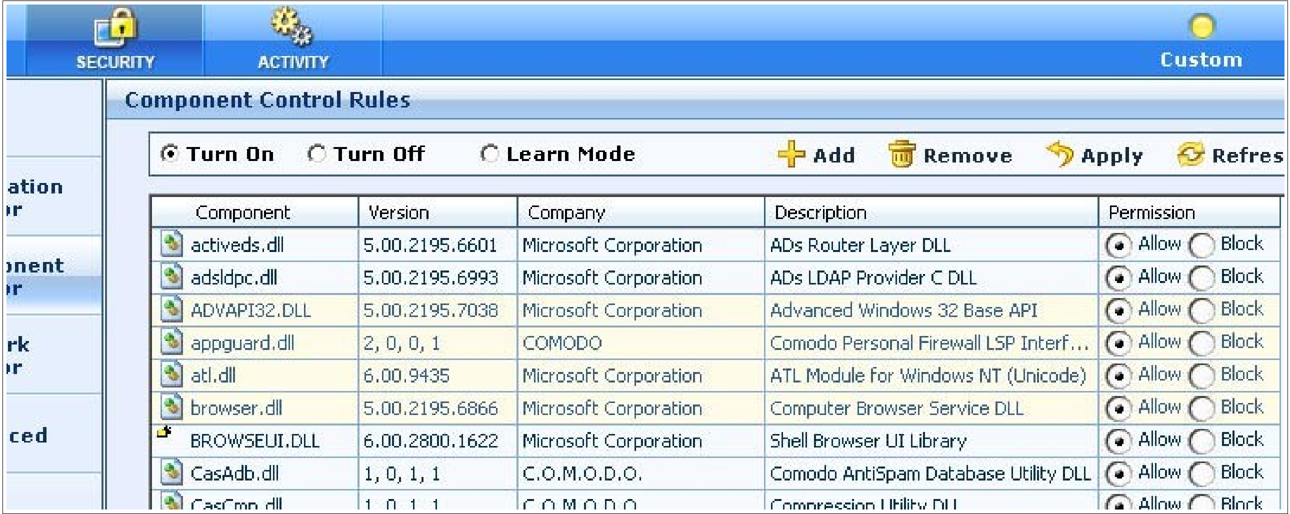
File name: ESigil.dll

Files of type: Library Files (*.dll)

☑ Open as read-only

After the rule is added, you can choose the permission to Allow or Block access.

Remove: Remove the selected components from the list



Component	Version	Company	Description	Permission
activeds.dll	5.00.2195.6601	Microsoft Corporation	ADs Router Layer DLL	● Allow ○ Block
adsldpc.dll	5.00.2195.6993	Microsoft Corporation	ADs LDAP Provider C DLL	● Allow ○ Block
ADVAPI32.DLL	5.00.2195.7038	Microsoft Corporation	Advanced Windows 32 Base API	● Allow ○ Block
appguard.dll	2, 0, 0, 1	COMODO	Comodo Personal Firewall LSP Interf...	● Allow ○ Block
atl.dll	6.00.9435	Microsoft Corporation	ATL Module for Windows NT (Unicode)	● Allow ○ Block
browser.dll	5.00.2195.6866	Microsoft Corporation	Computer Browser Service DLL	● Allow ○ Block
BROWSEUI.DLL	6.00.2800.1622	Microsoft Corporation	Shell Browser UI Library	● Allow ○ Block
CasAdb.dll	1, 0, 1, 1	C.O.M.O.D.O.	Comodo AntiSpam Database Utility DLL	● Allow ○ Block
CasCmp.dll	1, 0, 1, 1	C.O.M.O.D.O.	Compression Utility DLL	● Allow ○ Block

Select the component which you want to remove from the rules list and Click **Remove**.

Apply: Saves your settings after adding/removing components.

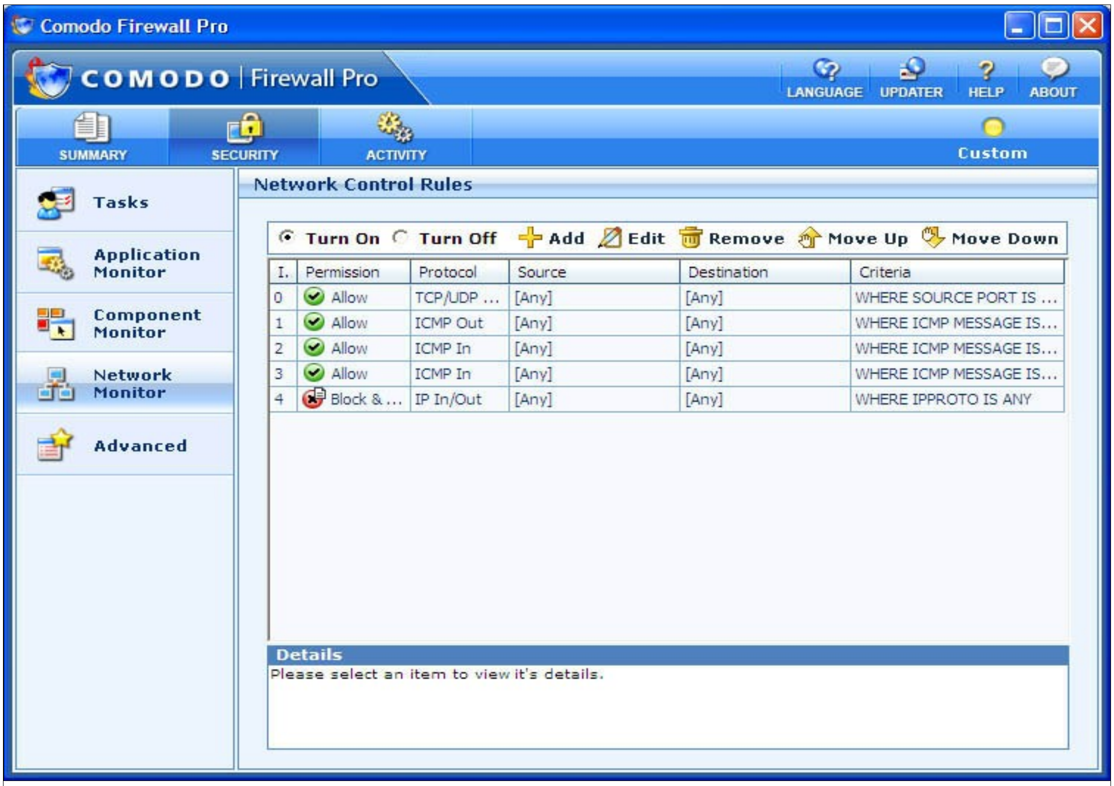
Refresh: When in learning mode, CPF continuously updates the component database which may not be reflected to component monitor list until Refresh button is pressed.

Network Monitor

Click on the ***Network Monitor*** tab in the Security main screen.

Network filtering rules can be added/modified/deleted through Network Control Rule Attributes. Any rules created using Add New Network Control Rule will be displayed in this list.

Comodo Firewall Pro applies rules on a *per packet* basis and applies the first rule that matches that packet type to be filtered. If there are a number of rules in the list relating to a packet type, the one nearer the top of the list will be applied.



I.	Permission	Protocol	Source	Destination	Criteria
0	Allow	TCP/UDP ...	[Any]	[Any]	WHERE SOURCE PORT IS ...
1	Allow	ICMP Out	[Any]	[Any]	WHERE ICMP MESSAGE IS...
2	Allow	ICMP In	[Any]	[Any]	WHERE ICMP MESSAGE IS...
3	Allow	ICMP In	[Any]	[Any]	WHERE ICMP MESSAGE IS...
4	Block & ...	IP In/Out	[Any]	[Any]	WHERE IPPROTO IS ANY

Details

Please select an item to view it's details.

Figure: Network Control Rules

Turn On/ Turn Off

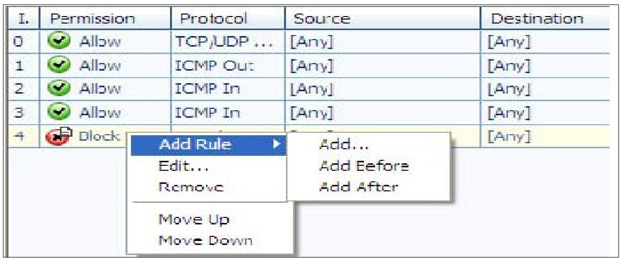
The radio buttons specify whether the violation of the listed rules generates an alert notification. The default and recommended setting is 'Turn On'.

Column Descriptions

1. The First Column ***(ID)*** represents the serial number of the applied network rule.
2. The Second Column ***(Permission)*** represents the action taken by the firewall, of either allowing or disallowing a network connection to be established.
3. The Third Column ***(Protocol)*** represents the direction of communication like incoming or outgoing and the protocol being used.
4. The Fifth Column ***(Destination)*** represents the IP Address of the computer accessing the network.
5. The Sixth Column ***(Criteria)*** represents the Port Numbers of individual applications.

Context Sensitive Menu

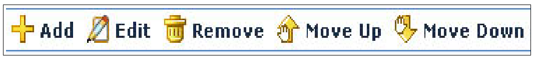
Rules can be modified by Right Clicking on any rule in the list. Comodo Firewall Pro then displays a context sensitive menu:



I.	Permission	Protocol	Source	Destination
0	Allow	TCP/UDP ...	[Any]	[Any]
1	Allow	ICMP Out	[Any]	[Any]
2	Allow	ICMP In	[Any]	[Any]
3	Allow	ICMP In	[Any]	[Any]
4	Block			[Any]

Shortcut Buttons

Alternatively, you can add,modify, remove, promote or de-escalate a network control rule by first selecting a rule then clicking on the desired button in the taskbar.



See below for more details on these actions.

Network Monitor Rule Configuration Options

Add Rule.. Adds a new Network Control Rule to the list.

Add Before... Adds the new rule above the currently selected rule.

Add After... Adds the new rule after the currently selected rule.

Edit... Allows the user to amend the network control rule options for the selected rule**.**

Remove... Deletes the currently selected rule.

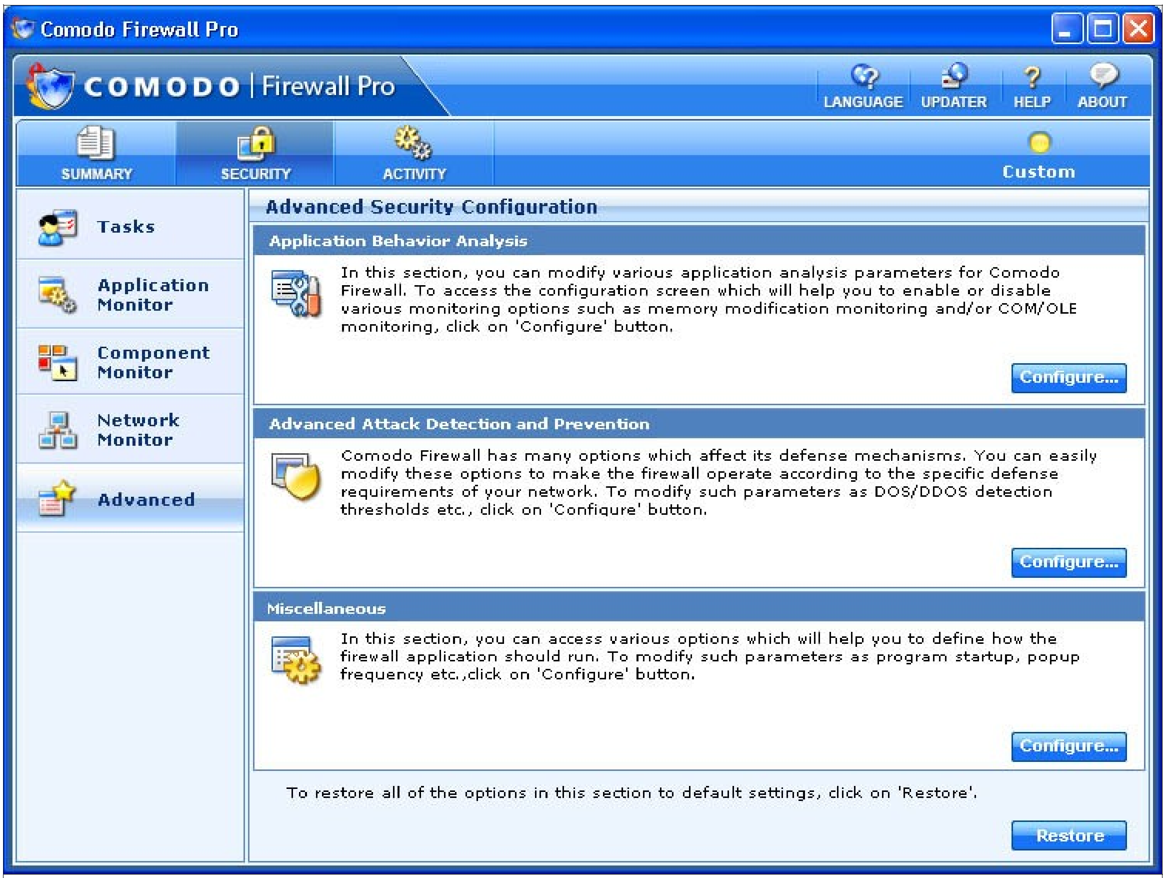
Move Up - Moves the currently selected rule up one row in the priority list.

Move Down - Shifts the currently selected rule down one row in the priority list.

Advanced Configuration

One of the key capabilities of Comodo Firewall Pro is Intrusion detection and intrusion prevention. It analyzes network packets and compares them with both known attacks and known patterns of attack, and then blocks those attacks. Advanced Configuration allows the user to configure the security settings at an advanced level.

In Advanced Configuration, you can configure the security settings at the following levels:



Advanced Security Configuration

Application Behavior Analysis

In this section, you can modify various application analysis parameters for Comodo Firewall. To access the configuration screen which will help you to enable or disable various monitoring options such as memory modification monitoring and/or COM/OLE monitoring, click on 'Configure' button.

Advanced Attack Detection and Prevention

Comodo Firewall has many options which affect its defense mechanisms. You can easily modify these options to make the firewall operate according to the specific defense requirements of your network. To modify such parameters as DOS/DDOS detection thresholds etc., click on 'Configure' button.

Miscellaneous

In this section, you can access various options which will help you to define how the firewall application should run. To modify such parameters as program startup, popup frequency etc.,click on 'Configure' button.

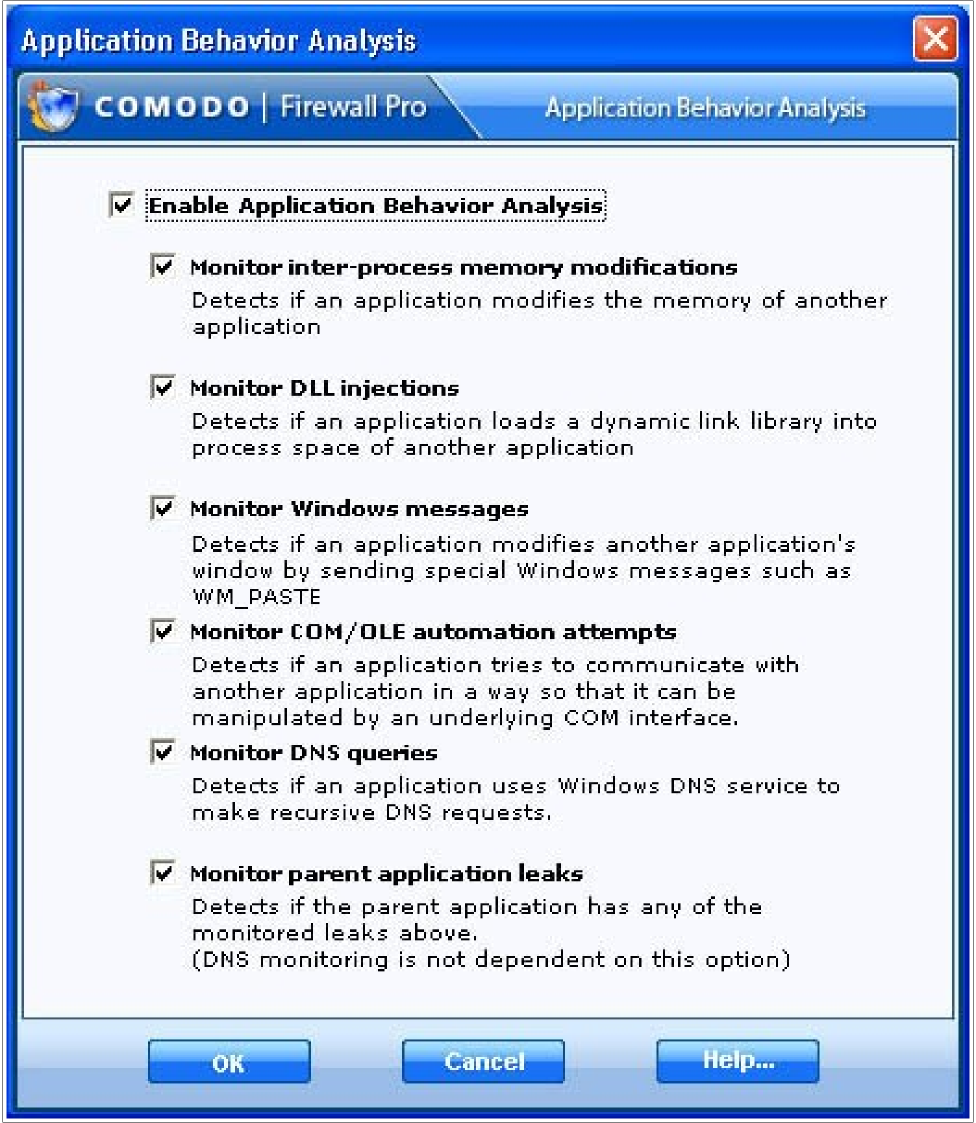
To restore all of the options in this section to default settings, click on 'Restore'.

Figure: Advanced Configuration

Application Behaviour Analysis

Comodo Firewall Pro analyses each application’s behavior and detects any suspicious activity before granting it internet access. This powerful new feature enables it to detect more trojan activity than any other firewall - the ultimate protection against the leaks that the most personal firewalls fail to detect, including:

- Process memory injections
- Invisible processes
- Parent application change
- DLL/Code injections



☑ Enable Application Behavior Analysis

☑ **Monitor inter-process memory modifications**
Detects if an application modifies the memory of another application

☑ **Monitor DLL injections**
Detects if an application loads a dynamic link library into process space of another application

☑ **Monitor Windows messages**
Detects if an application modifies another application's window by sending special Windows messages such as WM_PASTE

☑ **Monitor COM/OLE automation attempts**
Detects if an application tries to communicate with another application in a way so that it can be manipulated by an underlying COM interface.

☑ **Monitor DNS queries**
Detects if an application uses Windows DNS service to make recursive DNS requests.

☑ **Monitor parent application leaks**
Detects if the parent application has any of the monitored leaks above.
(DNS monitoring is not dependent on this option)

Enable Application Behaviour Analysis - Switches the functionality on or off

Monitor Inter-Process Injections Memory Modifications - Forces the firewall to monitor common code injection techniques that can be used by viruses

Monitor DLL Injections - Forces the firewall to monitor common DLL injection techniques used by viruses

Monitor Window Messages - Forces the firewall to monitor special window messages that can be used to manipulate an application’s behavior by a virus

Monitor DNS Queries - Forces the firewall to monitor DNS requests so that viruses trying to use Windows system services for DNS queries will be detected.

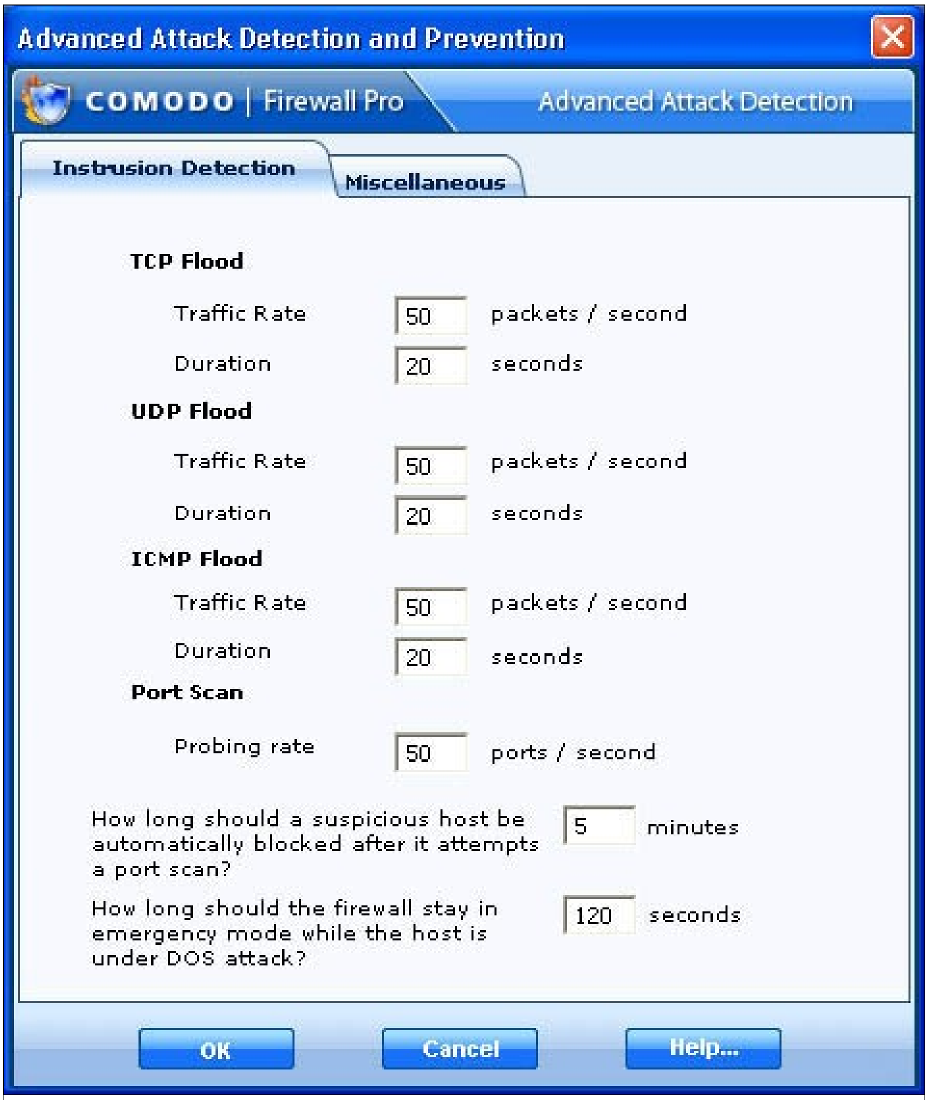
Monitor Parent Application Leaks - Forces the firewall to check if there is a leaking attempt in the parent application. i.e. if Process Injection is selected above, Comodo Firewall will look for the parent application to see if there is a process injection in it before allowing the internet request.

Monitor COM/OLE automation attempts - When enabled, forces the firewall to detect any program hijacking attempt which may occur by misuse of COM/OLE interfaces by other programs.”

Advanced Attack Detection and Prevention

'Intrusion Detection' tab

Comodo Firewall Pro Advanced Attack Detection protects against a common type of denial of service (DoS) attack used against servers. When launching a denial of service or 'flood' attack, an attacker bombards you with so many connection requests that your computer is unable to accept legitimate connections, effectively shutting down your web, email, FTP or VPN server. Comodo Firewall employs parameters to detect and protect you from flood attacks.



TCP Flood

Traffic Rate 50 packets / second

Duration 20 seconds

UDP Flood

Traffic Rate 50 packets / second

Duration 20 seconds

ICMP Flood

Traffic Rate 50 packets / second

Duration 20 seconds

Port Scan

Probing rate 50 ports / second

How long should a suspicious host be automatically blocked after it attempts a port scan? 5 minutes

How long should the firewall stay in emergency mode while the host is under DOS attack? 120 seconds

Figure: Intrusion Detection tab

Comodo Firewall Pro is capable of filtering traffic based on /TCP/UDP ports and packet types. It can be configured to accept limited traffic from specific addresses or completely prohibit all access. In addition, specific TCP/UDP traffic, or any application based on these protocols can be restricted. Advanced mechanism for flood detection, such as TCP flood, UDP flood and ICMP flood, allows for quick isolation of such malicious attacks.

TCP Flood / UDP Flood / ICMP Flood

Flood attacks happen when many packets of data are sent either via TCP, UDP or ICMP with a spoofed IP source address which will never send back a response to the destination server. This results in a backlog of responses. When this is done multiple times from multiple sources it floods the destination server, which has a limit of unacknowledged responses it can handle. This will ultimately bring down the server. By default, Comodo Firewall is configured to accept limited traffic for a set duration, for example, 50 packets per second for 20 seconds. If the packets threshold is exceeded, a DOS attack is detected and the Firewall goes into emergency mode. The firewall will stay in emergency mode for the duration set by user. By default this is set at 120 seconds. Users can alter this to their own preference by configuring How long should the host stay in emergency mode while the host is under dos attack (see below), by default, the duration is set to 120 seconds. In the emergency mode, all inbound traffic is blocked except those previously established and active connections. However, all outbound traffic is still allowed.

Ports Probe Rate

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 Pro detects the most common forms of port scans, alerting you and temporarily blocking the banning the IP address of the scanner, ensuring that they are "cut off" before they can discover any useful information about your system.

This is enabled by the Port Scan Probe Rate i.e. by default, when the number of individual ports scans exceeds 50 per second at your system; this pattern is detected as a port scan. This indicates that someone is scanning your system for services or vulnerabilities, Comodo Firewall will detect this as a port scan.

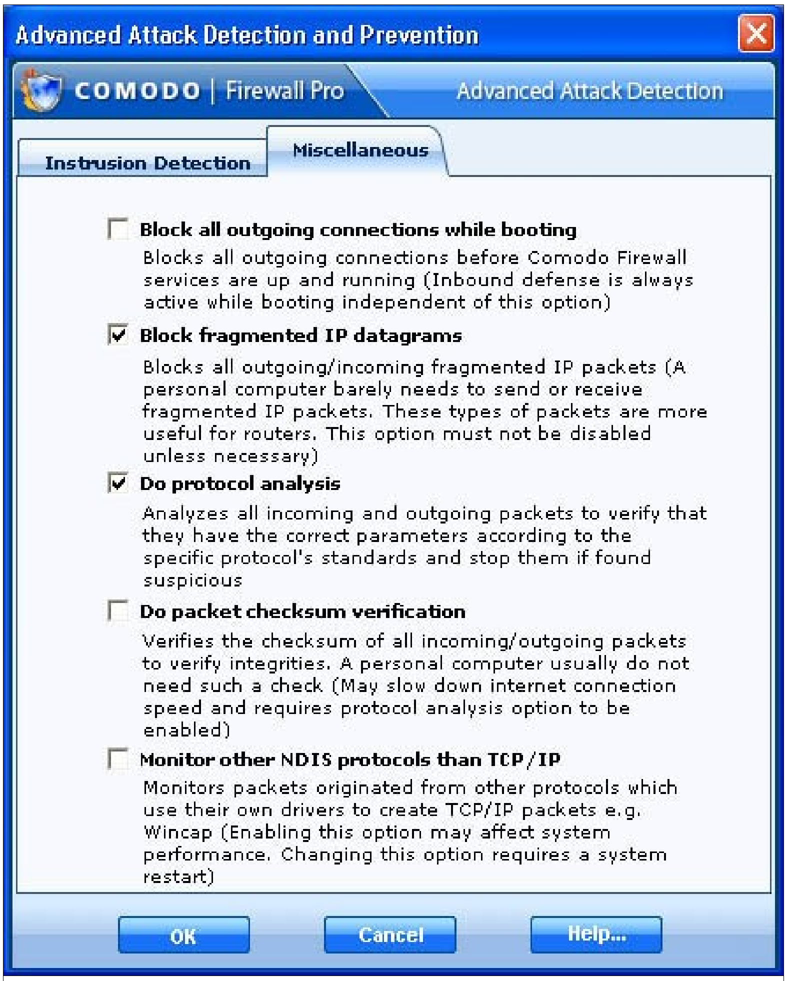
How long should a suspicious host be...

If a port san is detected, the Firewall identifies the host scanning your system as suspicious and automatically blocks its access for example 5 minutes, as set by default. During these 5 minutes, the suspicious host cannot access the user’s system but the user’s system can access it.

How long should the firewall stay in emergency mode...

When a DOS is detected, the Firewall goes into emergency mode for a duration , set by default to 120 seconds. During this stealth mode, the existence of your computer becomes 'invisible' as all inbound traffic is blocked for that duration. When your machine does not reply to network events, the sender is led to believe that there is no machine at the IP addresses which they're pinging. Hiding your machine's presence on the Internet is in some ways good from a security standpoint, because if a hacker thinks that your machine is not online, they may not make further attempts to access it.

'Miscellaneous' tab


Advanced Attack Detection and Prevention
COMODO | Firewall Pro
Advanced Attack Detection
Instrusion Detection
Miscellaneous

□ **Block all outgoing connections while booting**
Blocks all outgoing connections before Comodo Firewall services are up and running (Inbound defense is always active while booting independent of this option)

☑ **Block fragmented IP datagrams**
Blocks all outgoing/incoming fragmented IP packets (A personal computer barely needs to send or receive fragmented IP packets. These types of packets are more useful for routers. This option must not be disabled unless necessary)

☑ **Do protocol analysis**
Analyzes all incoming and outgoing packets to verify that they have the correct parameters according to the specific protocol's standards and stop them if found suspicious

□ **Do packet checksum verification**
Verifies the checksum of all incoming/outgoing packets to verify integrities. A personal computer usually do not need such a check (May slow down internet connection speed and requires protocol analysis option to be enabled)

□ **Monitor other NDIS protocols than TCP/IP**
Monitors packets originated from other protocols which use their own drivers to create TCP/IP packets e.g. Wincap (Enabling this option may affect system performance. Changing this option requires a system restart)

Figure: Miscellaneous tab

Block all outgoing connections while booting

This option allows the user to secure the host whilst booting by blocking all connection attempts until the system is up and running.

Block fragmented IP Datagrams

When a connection is opened between two computers, they must agree on a Mass Transmission Unit (MTU). IP fragmentation occurs when you pass through a router with an MTU less than the MTU you are using i.e when a datagram is larger than the MTU of the network over which it must be sent, it is divided into smaller fragments which are each sent separately. Fragemented IP packets can create threats like DOS attack. Moreover, these fragmentations can double the amount of time it takes to send a single packet and slow down your download time.

Comodo Firewall Pro 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 denial of service attacks. Checking this option means Comodo Firewall Pro checks every packet conforms to that protocols standards. If not, then the packets are blocked.

Do Packet Checksum Verification

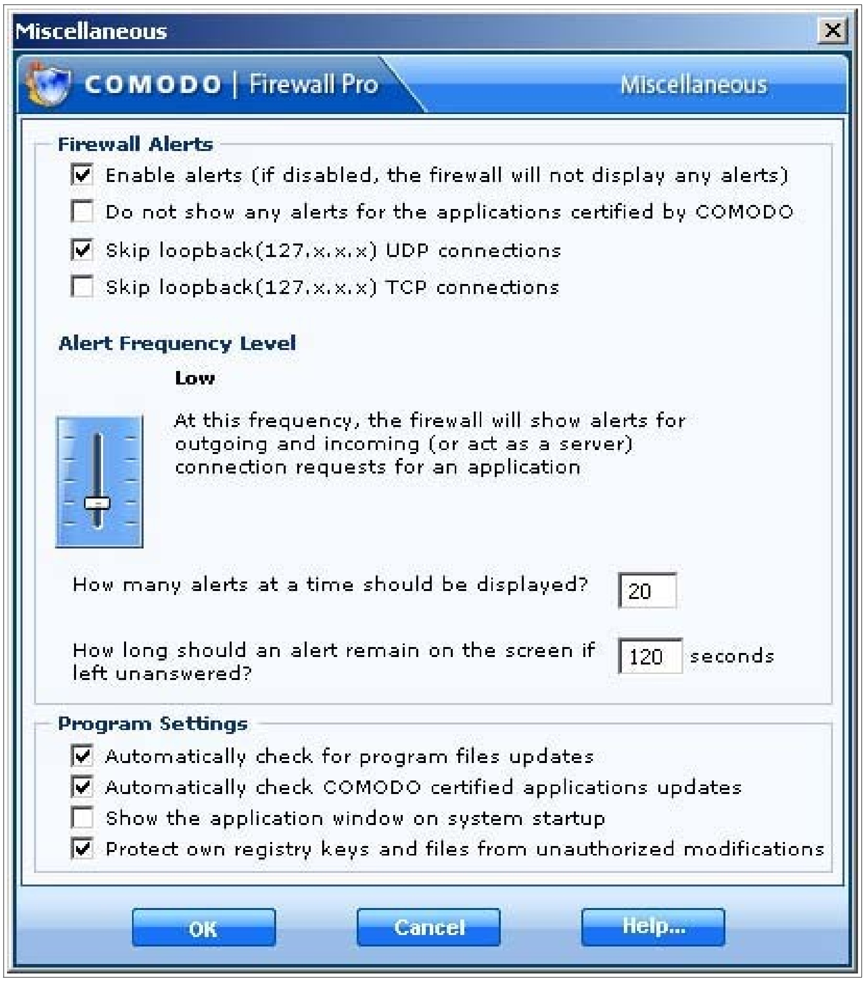
Every packet of data sent to your machine has a signature attached. With this option enabled, Comodo Firewall will recalculate the checksum of the incoming packet and compare this against the checksum stated in the signature. If the two do not match then the packet has been altered since transmission and Comodo Firewall will block it.

Monitor other NDIS protocols than TCP/IP

This will force Comodo Firewall to capture the packets belonging to any other protocol diver than TCP/IP. Trojans can 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.

Miscellaneous

The Miscellaneous section allows you to (1) Manage the generation of alerts in Comodo Firewall Pro (2) Configure various program settings.



Firewall Alerts

☑ Enable alerts (if disabled, the firewall will not display any alerts)
□ Do not show any alerts for the applications certified by COMODO
☑ Skip loopback(127.x.x.x) UDP connections
□ Skip loopback(127.x.x.x) TCP connections

Alert Frequency Level

Low

At this frequency, the firewall will show alerts for outgoing and incoming (or act as a server) connection requests for an application

How many alerts at a time should be displayed? 20

How long should an alert remain on the screen if left unanswered? 120 seconds

Program Settings

☑ Automatically check for program files updates
☑ Automatically check COMODO certified applications updates
□ Show the application window on system startup
☑ Protect own registry keys and files from unauthorized modifications

Firewall Alerts

Enable Alerts

Switches alerts on or off. Unchecking this option means no alerts will be generated by the program. Whilst this does not affect your security (which is determined by the rules that you have created for the firewall), it will diminish your awareness of connection attempts. Without alerts, any connection attempts that do not have any matching rules will be blocked but you will not be notified. However, in the case of serious attacks, this setting will be over-ruled and an alert generated. It is highly recommended that you leave this option checked and configure pop up frequency using the Alert Frequency Slider (see below)

Do not show alerts for applications certified by Comodo

This option automatically approves safe applications. When enabled, it forces the firewall to allow all activities of an application which is recognized as safe by its internal database of over 10000 applications. Unless explicitly blocked by a rule, the firewall will allow any activity of the safe applications while still watching for suspicious activities. The firewall will still raise an alert if it detects anything suspicious. This option is useful for avoiding unnecessary number of alerts.

Skip loopback (127.x.x.x) UDP connections

Loopback connections refer to the internal communcations within your PC. Any message transmitted by your computer through a loopback connection is immediately also received by it. This involves no connection outside your computer to the internet or a local network. This option is checked by default because the threat profile is very low for UDP attack using this channel whilst enabling would lead to a large increase in unnecessary alerts.

Skip loopback (127.x.x.x) TCP connections

Loopback connections refer to the internal communciations within your PC. Any message transmitted by your computer through a loopback connection is immediately also received by it. This involves no connection outside your computer to the internet or a local network. The TCP option is not checked by default because, in the case of someone using a proxy server, there is a higher chance of attacks being launched using a loopback connection.

Alert Frequency Level

Users can configure the amount of alerts that Comodo Firewall generates with this slider. Raising or lowering the slider will change the amount of alerts accordingly. It should be noted that this does not affect your security, which is determined by the rules you have configured. For the vast majority of users, the default setting of 'Low' is the perfect level - ensuring you are kept informed of connection attempts and suspicious behaviours whilst not overwhelming you with waves of alerts.

How many alerts at a time should be generated?

The user can configure the generation of a maximum number of alerts to be generated at one time. By default, the maximum number of alerts is kept at 20 appearing as Alert 1 0f 20, 2 of 20 and so on. The pop-up window will include a navigation bar if the number of alerts is greater than one and the alerts are stored in the memory so that the user can navigate between them until they are responded to.

How long should an alert remain on the screen if left unanswered

Determines how long the Firewall will show an alert for without any user intervention. By default, the timeout is set at 120 seconds.

For an in depth explanation of the types of alerts and how to understand them, please refer to Alerts

Program Settings

Automatically check for program file updates

Determines whether or not Comodo Firewall Pro should automatically contact Comodo servers for updates. We advise users enable this option to maintain the highest level of protection. Users that choose to disable automatic updates can manually download updates by clicking the 'Updater' button at the top right of the firewall interface.

Automatically check Comodo certified application updates

This option allows the user to update Comodo Firewall Pro's internal database of known applications from our servers on a daily basis. It is highly recommended users keep this setting to it's default 'Checked' status.

Show Application window on system start up

The start or 'splash' screen of the firewall appears every time you re-start your computer. Furthermore, by default settings, the main window of the firewall will be opened every time you re-start your computer. If you do not wish to see the application window on system start-up, just uncheck the Show Application Window on System Start Up box.

Protect own registry keys and files from unauthorized modifications

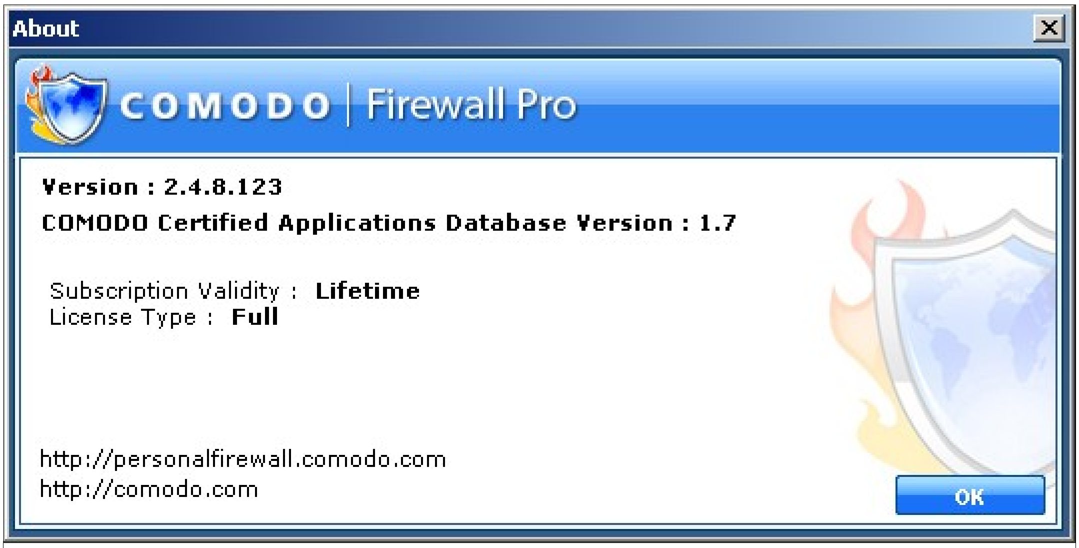
Meaning that Comodo Firewall Pro registry entries and files cannot be deleted or modified either accidentally or deliberately. This vital security feature prevents malicious programs or intruders from being able to shut down or sabotage your installation of Comodo Firewall Pro. Leaving this option checked will protect your system from:

- Malicious trojan horse programs and spyware - The first thing a burglar does when he breaks in to a house is to switch the alarm off. To avoid detection, many trojan horse programs follow the same logic and attempt to modify or remove the user's firewall. This feature prevents any such attacks.
- Manual deletion or modification. User interaction with Comodo Firewall libraries and files is disabled. e.g. A user cannot accidentally delete firewall registry keys using utilities such as Windows RegEdit. Similarly, a hacker is not able to disable or delete critical firewall system files such as 'cpf.exe'.

About Comodo Firewall

Clicking the 'About' tab on the Comodo Firewall Pro Summary page to view the 'About' information dialog.

From here you can view information about the Version Number of the Firewall that is installed on your computer , the Web site from where you can download the latest version of the Comodo Firewall Pro and the status of your license like Subscription validity and the type of License .



Version : 2.4.8.123
COMODO Certified Applications Database Version : 1.7

Subscription Validity : Lifetime
License Type : Full

http://personalfirewall.comodo.com
http://comodo.com

Figure: About Comodo Firewall Pro

For more information, you can visit the site :http://www.personalfirewall.comodo.com and http://www.comodo.com/.

About Comodo

Comodo is a leading global provider of Identity and Trust Assurance services on the Internet, with over 200,000 customers worldwide. Headquartered in Jersey City, NJ with global offices in the UK, Ukraine, and India, the company offers businesses and consumers the intelligent security, authentication and assurance services necessary to ensure trust in online transactions.

As a leading Certification Authority, and in combination with the Digital Trust Lab (DTL), Comodo helps enterprises address digital ecommerce and infrastructure needs with reliable, third generation solutions that improve customer relationship, enhance customer trust and create efficiencies across digital ecommerce operations. Comodo's solutions include SSL certificates, integrated Web hosting management solutions, web content authentication, infrastructure services, digital ecommerce services, digital certification, identity assurance, customer privacy and vulnerability management solutions.

Comodo is delivering the highly rated Comodo Firewall Pro free to consumers as part of an initiative to empower consumers to create a safe and trusted online experience whenever they go online. This initiative will make available free to all consumers some of the leading tools that consumers can use to be safe and avoid leading threats such as Phishing attacks.

To download Comodo Firewall Pro and other free security products, visit
http://www.Comodogroup.com/products/free_products.html

Getting Support

Need Help?

Comodo Forums

The fastest way to get further assistance on Comodo Firewall Pro is by joining Comodo Forums, a message board exclusively created for our users to discuss anything related to our products. Register free at http://forums.comodo.com

You'll benefit from the expert contributions of developers and fellow users alike and we'd love to hear your thoughts and suggestions.

Users can also access the forums by clicking "Need Help?" in the 'Tasks' main screen.

Online Knowledge Base

We also have an online knowledge base and support ticketing system at http://support.comodo.com . Registration is free.