

Quick Heal

QUICK START GUIDE

Quick Heal Firewall Pro 3.0

Quick Heal Technologies (P) Ltd.

<http://www.quickheal.com>

ABSTRACT

This document provides a quick start reference to familiarize a first time user in the basic concepts and operations of Quick Heal Firewall Pro 3.0 software. It also gives some of the primary ways a user might want to customize Quick Heal Firewall Pro to fit his or her preferences.

TABLE OF CONTENTS

SOME BACKGROUND	4
INTERNET BASICS	4
WHY QUICK HEAL FIREWALL PRO IS NEEDED?	4
THE MAIN THREATS.....	5
HOW QUICK HEAL FIREWALL PRO WORKS.....	5
QUICK HEAL FIREWALL PRO'S FEATURES.....	5
GETTING STARTED	6
SYSTEM REQUIREMENTS.....	6
INSTALLING QUICK HEAL FIREWALL PRO.....	6
UNINSTALLING QUICK HEAL FIREWALL PRO	13
USING QUICK HEAL FIREWALL PRO	14
INITIAL OPTIONS	15
OPERATIONAL MODES	15
RULES WIZARD	17
ADVANCED SETTINGS	18
SAFEGUARDING YOUR SYSTEM	18
PREVENTING NETWORK ATTACKS	21
SETTING A PASSWORD.....	23
TECHNICAL SUPPORT	24

SOME BACKGROUND

INTERNET BASICS

The Internet is interactive, which simply means that when a computer is connected to the Internet, data can be sent and received by that computer to other computers on the Internet. This interactivity is built into the Internet and is a fundamental part of it.

To see a web site on the Internet, your computer basically asks that site for its files. The site's computer (server) then sends (serves) those files to your computer. For the files to get from the server all the way through the Internet over to your computer, your computer must give the site's server your computer's address. This address is unique and called IP address. No other computer on the Internet has this same address.

The Internet uses what's called a server-client way of doing things. Web sites use servers to supply their web pages and people use their computers as clients that are served those pages. The vast majority of information on the Internet goes from the servers to the clients, from the web sites to the desktop computer. Very little information goes from your computer back to the server.

WHY QUICK HEAL FIREWALL PRO IS NEEDED?

The major reason Quick Heal Firewall Pro is needed is because a small percentage of Internet users are destructive. These people are called hackers or crackers. Traditionally a hacker is an accomplished computer programmer who is an expert in networks. A cracker is the term for someone who gains unauthorized access to a computer or system. The news media has blurred these definitions and refers to anyone who breaks into other people's computers as a hacker. It used to take some skill to crack into a system but nowadays there are programs that can do it automatically. Children without much training or expertise can use them. These programs can be gotten effortlessly from the Internet. Many of these programs are sent around the Internet haphazardly as attachments to e-mails. Once the program is running on a user's machine, it "calls home" to a central site and reports where it is. The hacker can then control that user's machine remotely without the user even being aware of it. The hacker can record all the keyboard actions and mouse movements of the user's computer so can capture credit card data and passwords with ease. Sounds like science fiction but it is very much a cold, hard fact.

Another undesirable element of the Internet is the ever-present threat of computer viruses that are disseminated through email. These are so numerous that if something goes wrong with a computer the first thing suspected (and often discovered) is a virus.

Advertiser tracking of your surfing habits and interests has recently become a concern of privacy advocates. Advertisers use the data they gather on you to push specific ads calculated to increase your purchasing.

THE MAIN THREATS

- Someone on the Internet thousands of miles away can access your computer and personal files more easily than your neighbor down the street.
- Once your computer is accessed, all of its files can be viewed, copied and erased.
- Your computer can be used to attack other innocent user's computers without your knowledge.
- A hacker can very easily make your Internet connection totally unusable just for kicks.
- Your passwords, credit card information, house address can all be obtained remotely very easily.
- Unscrupulous advertisers can track your surfing habits, your interests and your locale, thereafter target specific ads at you.
- Your Personal information can be collected for various reasons, all without your knowledge or consent.

HOW QUICK HEAL FIREWALL PRO WORKS

Quick Heal Firewall Pro is a firewall, the technical name for a barrier between your computer and the rest of the Internet. It's like the lock on the doors of your home. Most of your neighbors can probably be trusted not to walk into your home and vandalize it or steal from you. Usually only a small number of your neighbors are untrustworthy. But, if you live in heavily populated area, there are a greater number of dishonest people around.

The Internet is similar except that your immediate neighborhood consists of hundreds of millions of people. Even the small percentage of those people who have a destructive bent is a large number of people.

Quick Heal Firewall Pro not only locks your computer's "doors", it makes your computer invisible on the Internet. Your computer normally lets other Internet users know its address. It's like the address sign of your home or the license plate of your car. Your computer's address is plainly visible. Quick Heal Firewall Pro prevents your computer from broadcasting its address unless specifically authorized by you. Hackers are not just kept out; they cannot find out that your computer is connected to the Internet.

QUICK HEAL FIREWALL PRO'S FEATURES

- Starts protecting immediately after being installed.
- Has a default configuration setting for new users.
- During the installation auto-configures for optimum protection.
- Can be customized in detail by advanced users.
- Makes your computer invisible on the Internet.
- Locks your computer's "doors" ports against intrusion.
- Let's you decide how much an application should be trusted.
- Uses plug-ins to increase its power while keeping the same familiar interface.
- Prevents your computer from being controlled remotely.
- Notifies you of any hidden software attempting to "phone home" to a hacker.
- Runs on all recent versions of Windows so can still be used if you upgrade.
- Uses very little system resources so does not noticeably affect your computer's performance.
- Advanced Log System lets you view any event on your system.
- Successful on all known "leak-tests".

GETTING STARTED

SYSTEM REQUIREMENTS

The minimum system requirements for Quick Heal Firewall Pro are:

- 450 MHz Intel Pentium or compatible CPU
- 256 MB RAM
- 32-bit and 64-bit versions of Windows XP/Windows 2003/Windows Vista/Windows 2008/Windows 7 operating system
- 150 MB of free hard disk space.

INSTALLING QUICK HEAL FIREWALL PRO

IMPORTANT WARNING

Shutdown and uninstall any other firewall software before installing Quick Heal Firewall Pro on your computer. Trying to install a firewall over other running firewall software will crash your computer.

Once you are certain no other firewall is operating on your computer, install Quick Heal Firewall Pro by running **QHFVPRO.exe**. It is recommended that you use the default settings when the installation utility asks you to confirm its choices if you are not an advanced user.

The setup wizard contains several steps. Each step has a **Next** button that takes you to the next step of the procedure, a **Back** button that returns you to the previous step and a **Cancel** button that exits the wizards and aborts the entire setup procedure.

After clicking the **Next** button you will be asked to accept the License Agreement to use the **Quick Heal Firewall Pro**.



Figure 2-1: Welcome to the Quick Heal Firewall Pro Setup Wizard

Please read it carefully. This dialog's **Next** button is enabled only if you select the option button **I accept the agreement** indicating that the License Agreement is acceptable to you

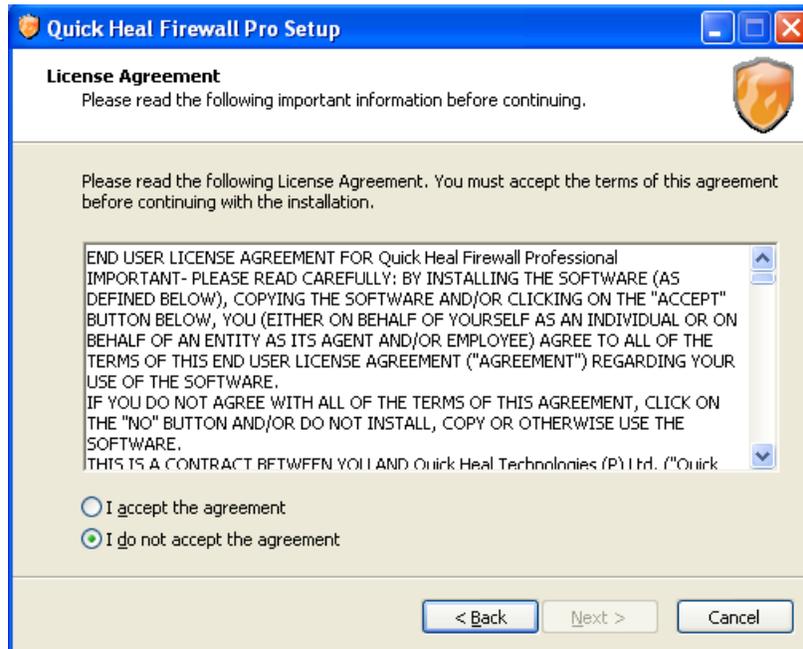


Figure 2-2: License Agreement

After you have accepted the License Agreement, the Next button brings you to the **Select Destination Location** step

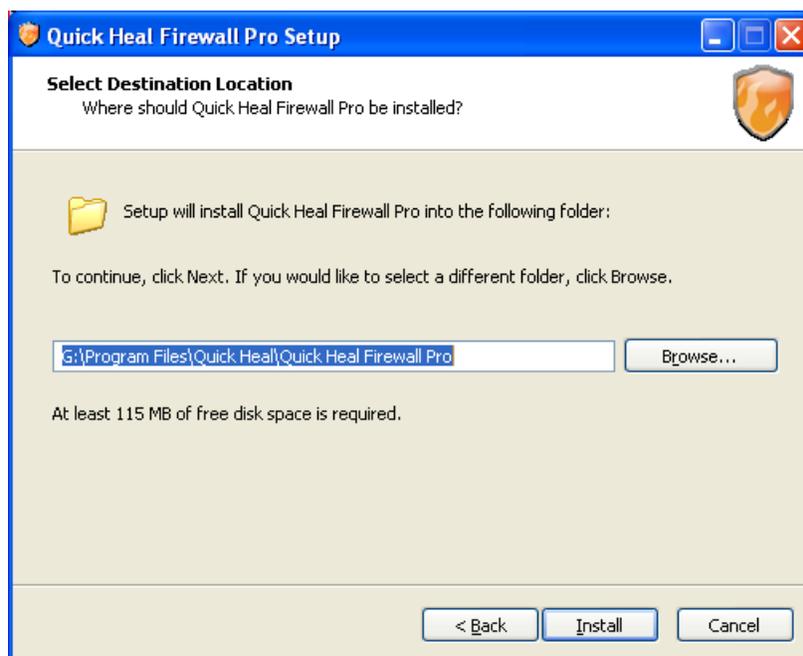


Figure 2-3: Select Destination Location

Select a folder where you want to install Quick Heal Firewall Pro files. You can use the default folder or select it manually.

If you want to change the default file location, click Browse. Select the folder or create your own one and click OK. Click Next to proceed to the last step before actual installation. If you need to cancel any performed steps, click **Back**. When you are ready to go ahead with the installation, click the **Install** button.

The program displays the installation progress window

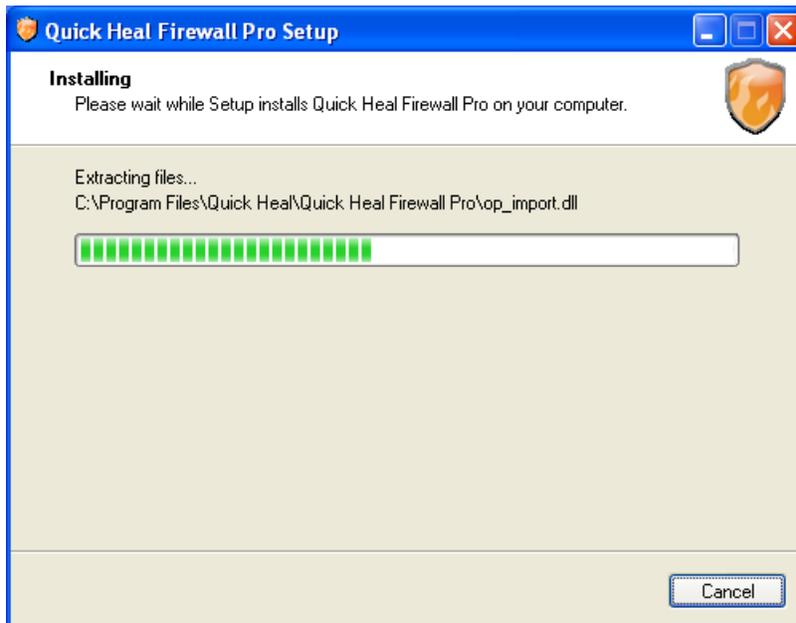


Figure 2-4: Installation Progress

After the installation is finished, a new configuration setup wizard will offer you to select a necessary security level



Figure 2-5: Specify Security Level

Advanced security provides the highest level of security and protects against all penetration techniques that are often used by malicious programs to bypass firewalls. Normal security protects against the most dangerous penetration techniques. It decreases a number of product prompts for users to reply on and is recommended in most cases.

Select the desired level to proceed to the step. Quick Heal firewall Pro automatically scans your system and adjusts all its settings without your supervision. It configures network settings, builds the Component Control database, and, in case you select to use predefined rules, searches for known applications installed on your computer that might require Internet access and configures an appropriate the network access level for each of them:

Click **Finish** to apply the changes and save the configuration. You will be asked to reboot your system



Figure 2-6: Installation Complete

! Do not launch Quick Heal Firewall Pro manually using the Start button menu or Windows Explorer right after installing it. You must reboot your computer before Quick Heal Firewall Pro start to protect your system.

UNINSTALLING QUICK HEAL FIREWALL PRO

To uninstall Quick Heal Firewall Pro:

1. Right click the Quick Heal Firewall Pro system tray icon and select **Exit**.
2. Click **Start** on the Windows taskbar and select **Control Panel > Add or Remove Programs**.
3. Select **Quick Heal Firewall Pro** and click **Remove**.
4. Click **Yes** to confirm the removal.

All the necessary actions will be performed automatically. Afterwards you will be prompted to restart your system.



To avoid program conflicts restart the system after the removal process is completed.

USING QUICK HEAL FIREWALL PRO

To start Quick Heal Firewall Pro, click **Start** -> **Programs** -> **Quick Heal Firewall Pro** -> **Quick Heal Firewall Pro**. The main window looks as follows:

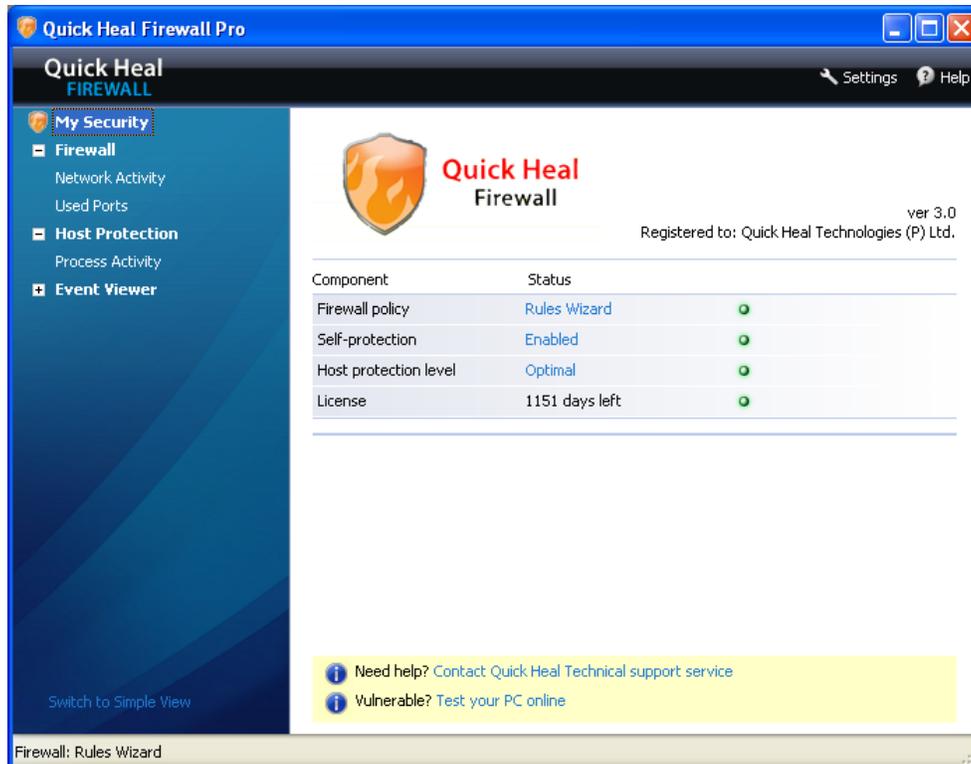


Figure 2-7: Quick Heal Firewall Pro Main Window

To exit from Quick Heal Firewall Pro, right click the Quick Heal Firewall Pro icon in the system tray and click **Exit**.

INITIAL OPTIONS

OPERATIONAL MODES

By default, Quick Heal Firewall Pro is automatically loaded when your computer starts up providing immediate protection with the earliest stage possible. Once it is loaded, the default icon with the orange shield  is displayed in the windows system tray. When you see the icon, it means that Quick Heal firewall Pro is operating and protecting your system.

For any reason to completely stop the Quick Heal Firewall Pro, right-click the Suite's icon in the system tray, click Exit, select Exit Quick Heal Firewall Pro and shutdown service from the list and click OK.

Startup Mode

Quick Heal Firewall Pro allows to control its behavior when system start up. To select one of the three startup modes, click the Settings button on the toolbar. The following modes are available on the General page under the Operation settings section:

- **Normal** – The default mode. Loads Quick Heal Firewall Pro automatically when the system is turn on and displays its icon in the system tray.
- **Background** – In background startup mode, Quick Heal Firewall Pro runs without displaying icon in windows system tray. This makes the suite invisible to users, blocks unwanted traffic or content in a way that's completely hidden from the user.
- **Disable** – If this mode is selected, Quick Heal Firewall Pro will not run automatically at startup. System will not be protected until you manually start Quick Heal Firewall Pro.

Quick Heal Firewall Pro gives a wide choice of protection levels all the way from totally blocking all Internet access of every application on your computer to allow full access to every application. For your convenience, Quick Heal Firewall Pro has different operational modes to conform to the protection level you prefer.

Selecting the Firewall Policy

- **Block all** — all network connections are disabled.
- **Block most** — all network connections are disabled except those apps you enable.
- **Rules Wizard** — you enable or disable apps when they are first run.
- **Allow most** — all network connections are enabled except those apps you disable.
- **Disable** — all network connections are enabled.

The default policy is Rules Wizard. Quick Heal Firewall Pro icon in the system tray shows Quick Heal Firewall Pro's mode. To change the Firewall Policy:

1. Right-click the system tray icon
2. The following menu appears. Go to **Firewall Policy** and select the desired policy by clicking it.

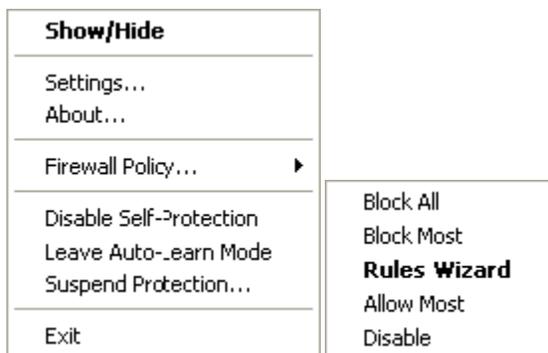


Figure 3-1: Right Click Firewall Policy

Changing the Firewall Policy

To change the current firewall policy:

1. Click **Settings** on the toolbar.
2. Select the **Firewall**.
3. Select the desired policy by moving the slider up or down and click **OK**.

To completely disable the firewall, clear the **Enable firewall** box.

Tip:

- You can also change the firewall policy using the system tray icon's shortcut menu. Right click the icon, select Firewall Policy and select the desired policy from the menu.



If the firewall is disabled, attack detection is also disabled.

Running in stealth mode

By default Quick Heal Firewall Pro runs in stealth mode which means that your computer does not respond to port scans and silently blocks them, making itself invisible to hackers. In stealth mode, computer will not respond as it is not turned on or not connected to the internet.

To switch the stealth mode, click **Settings** on the toolbar, select the **Firewall** tab and select/clear the **Run in stealth mode** check box.

RULES WIZARD

Rules Wizard is the operational mode that lets you decide each application's permissions to use the Internet. Quick Heal Firewall Pro asks you whenever an application (app) first tries to send or receive data. Rules Wizard is the default operational mode and is recommended for most users. You can choose to make a rule for an app. If a rule is made then Rules Wizard is not displayed again for that app. If no rule is made for an app then Rules Wizard will display again the next time that app tries to send or receive data.

Don't be concerned about setting rules for application. You can easily change or delete an application's rules at any time.

It shows you the application (Internet Explorer, in this example), whether the application wants to send or receive data, the type of service the app is attempting to establish and the address the data is about to go to or be received from.

You are then given the following choices

Allow all activities for this application — for applications you trust completely. The application is then included in the Trusted applications list. (See **Settings** -> **Applications Rules**).

Block all activities for this application — for applications which you know should not have network access. The application is included in the Blocked applications list. (See **Settings** -> **Applications Rules**).

Create rule using preset — Quick Heal Firewall Pro lets you create rules using presets for most common applications or the presets that best suit an application (Internet Explorer, in our example above). Quick Heal Firewall Pro is designed to offer the preset that best suits your application. The application will be included in the partially allowed applications list. (See **Settings** -> **Applications Rules**). It is recommended that you select the preset offered by Quick Heal Firewall Pro; however advanced users can click on the drop-down menu and select other presets or even create their own rule sets by selecting **Other**.

Allow Once — for applications of which you are doubtful. The next time this application tries to establish a network connection, the same warning is displayed. No rule is created for the application.

Block Once — for applications of which you are uncertain and distrust. The next time this application tries to establish a network connection, the same warning is displayed. No rule is created for the application.

ADVANCED SETTINGS

SAFEGUARDING YOUR SYSTEM

Trojan horses are the most dangerous threats to your computer files and your confidential information such as your passwords, credit card data and personal correspondence. A Trojan is a program installed on your computer that gives full access to hackers. The same Trojan can be used secretly by many hackers. It's not just one Trojan to one hacker. It's one Trojan to many hackers.

A Trojan on your computer can let a hacker view, copy or erase any folder and any file on your computer just as though he or she were sitting at your computer using its keyboard and mouse. Any file on your computer can also be sent to any e-mail address or posted on the Internet.

There are many ways a system can be infected with a Trojan and because a Trojan is not the same as a virus. It is a self-replicating program segment and it is not always detected by antivirus software. Quick Heal Firewall Pro was designed to nullify the malicious actions of Trojans.

Quick Heal Firewall Pro's settings for maximum protection

- Rules Wizard mode informs you of any program trying to send data to or from your computer.
- Stop all mode prevents any data from being transmitted to or from your computer and Internet. Switch to this mode when you are absolutely certain that you don't need to access Internet resources, but still want to stay connected to the Web.
- Make your computer invisible to hackers. Click the **Settings** -> **Firewall**. Select the **Stealth** mode in the **Enable Firewall** field.
- Ensure NetBIOS is turned off (disabled) unless your computer is on a local network and needs to share its files. If you need to use NetBIOS press the Settings in the LAN Settings field and make sure NetBIOS is selected for your local network like shows the picture below:

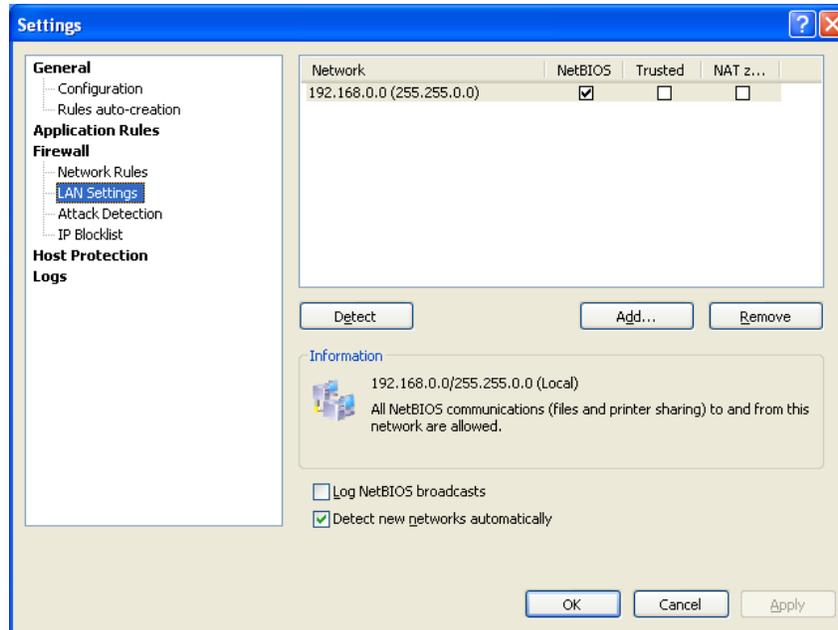


Figure 4-1: LAN Settings

Click **Add** to add a remote computer or network to the list of allowed NetBIOS communications. The following dialog will be displayed:

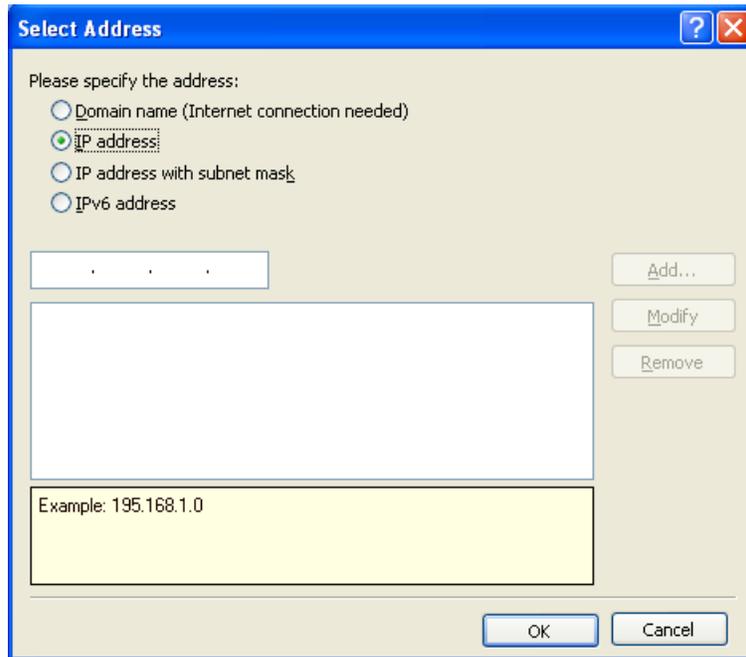


Figure 4-2: Selecting Address

To add a specific computer to the list, you must know its IP-address. Type either the domain name, IP-address, or subnet mask into the corresponding field. Each option suggests the required format. Please note that you must pay attention to this option because allowing unrestricted NetBIOS communications may result in severely decreased system security level.

PREVENTING NETWORK ATTACKS

A major function of firewall protection is inbound filtering, which controls all incoming activity to block hackers and malicious programs when they try to attack your computer.

Attack Detection component detects, prevents, and reports all possible attacks on your computer from the Internet or the network your computer is connected to. Attack Detection component can detect not only every one known type of attack (such as port scanning, Denial of service (DoS) and many more) but future exploits as well.

To enable Attack Detection component, click **Settings** on the toolbar, select the **Firewall** tab and select the **Enable Attack Detection** check box:

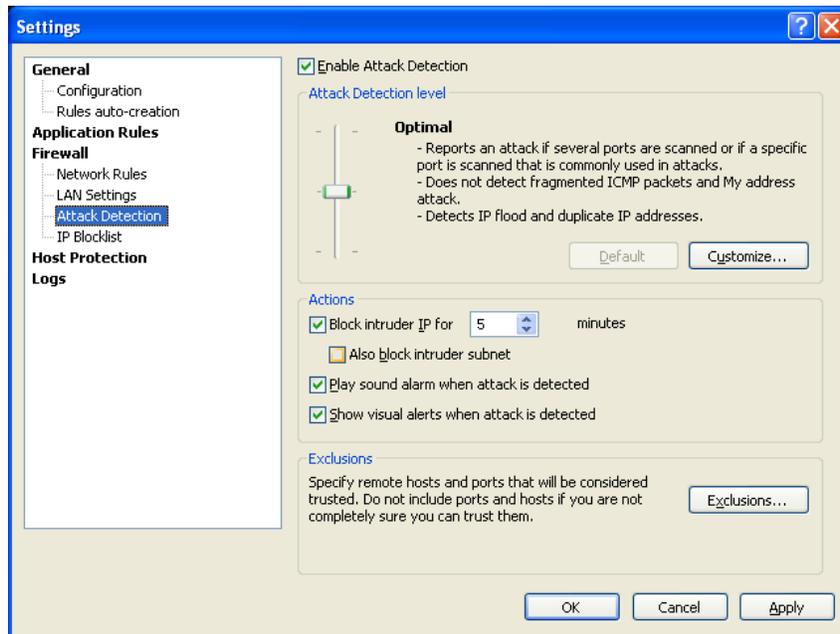


Figure 4-3: Network Attack Detection Settings

Specifying Attack Detection Level

You can define how sensitive Quick Heal Firewall Pro should be in detecting attacks by setting the desired attack detection level. Attack detection level determines the types of attacks to be detected and the number of suspicious packets received Quick Heal Firewall Pro reports a port scanning attack. To set attack detection level, click **Settings** -> **Attack Detection** and move the slider to one of the following values:

- **Maximum:** A port scan alert is displayed even when a single scan of one of your ports is detected. All Ethernet and external attacks are monitored for and prevented.
- **Optimal:** A port scan alert is displayed only when several ports are scanned or if a specific port is scanned that Quick Heal Firewall Pro recognizes as one commonly used in attack. All external attacks are monitored for except fragmented ICMP and My Address attacks.
- **Low:** A port scan alert is displayed only when a multiple scanning is definitely detected. Fragmented ICMP, My address and all Ethernet attacks are not monitored.

Change the attack detection level depending on the risk your computer is under or if you are suspicious, set the level to maximum.

You may also customize the security level to better meet your requirements by clicking the **Customize** button. The **Ethernet** tab lets you specify settings for Ethernet attacks, the **Advanced** tab will help you define a list of attacks detected by the firewall.

After Quick Heal Firewall Pro detects an attack, it can change its behavior to automatically protect you from any future attacks from the same address. To do this, select the **Block intruder for ... minutes** check box and all traffic from the computer yours will be blocked for the number of minutes you designate. The default value is 5 minutes.

You can also set to block the entire subnet the attackers address belongs to by selecting **Also block intruder subnet**.

To receive visual and/or sound alerts about detected attacks, select the **Show visual alert when attack is detected** and/or the **Play sound alarm when attack is detected** check boxes under Actions.

Specifying Trusted Hosts and Ports

There may be computers that you are absolute sure are not a source of danger to your system. The attack detection component features exclusion lists to which you can add hosts and ports you don't want to be monitored.

To add a host, a subnet or port to the trusted list, click **Settings -> Attack Detection -> Exclusions**.

Running in Self Protection Mode

As anti-malware tools have grown stronger, hackers now try to switch them off using rootkits and other advanced tools before proceeding with their own unauthorized actions. To withstand this threat, Quick Heal Firewall Pro features with Self-protection mode. With self-protection on, Quick Heal Firewall Pro protects itself against termination caused by viruses, Trojans or spyware. Quick Heal Firewall Pro also constantly monitors its own components on the hard drive, registry entries, memory status, running services and so on and disallows any changes by malicious applications.

By default, self-protection is enabled. To disable it, click the **Self-Protection** button on the toolbar.



Disabling self-protection may severely impact overall system security. Though disabling is required for the installation of plug-ins and other advanced functions, it should be re-enabled as soon as the changes have been made.

SETTING A PASSWORD

Quick Heal Firewall Pro enables you to protect the settings you specify from being altered without your permission. Being secured by a password, product settings cannot be changed by another person. For example, you can block access to objectionable sites for and your settings cannot be tampered with.

Setting the password

To set the password, click **Settings** on the toolbar, select the **Configuration** page and select the **Enable password protection** check box:

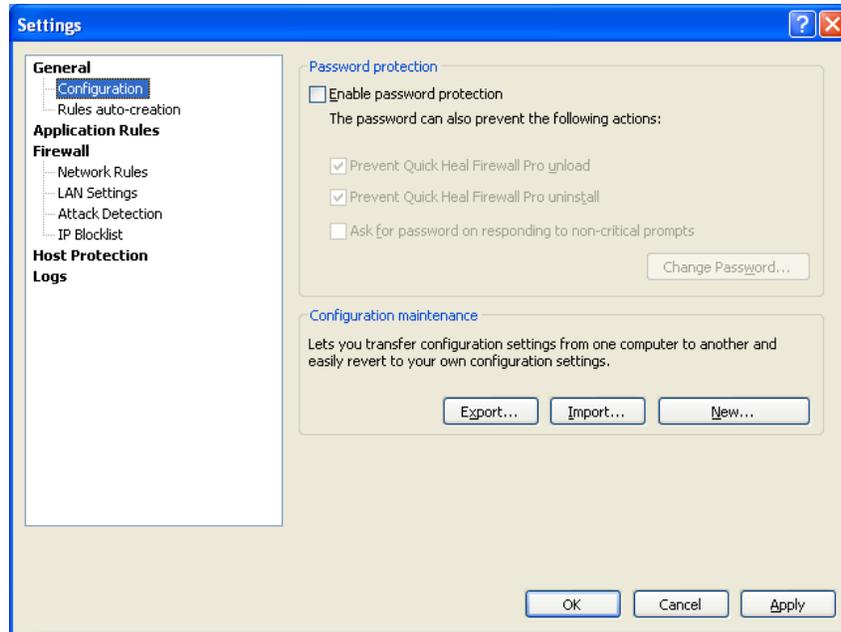


Figure 4-4: Password Settings

Specify the password in its dialog box, confirm it and click **OK** to save it. Click **OK** and Quick Heal Firewall Pro will start to protect its settings. If anyone tries to gain access to the product settings or to create a new configuration, prompt will be displayed for the password.

Changing the Password

To change the password, click **Settings** on the toolbar, select the **Configuration** page and click **Change Password** under **Password protection**. Specify and confirm the new password, then click **OK**.

Disabling the password

To disable the password, click **Settings** on the toolbar, select the **Configuration** page and clear the **Enable password protection** check box. After you click **OK** twice, all firewall settings will be available to every person who uses the computer.

Select the **Ask for password on responding to product prompts** check box if you want Quick Heal Firewall Pro to prompt for the password when a user responds to the Rules Wizard and Host Protection dialogs.



Please remember your password. If you forget the password, you will have to reinstall Quick Heal Firewall Pro or even your operating system.

TECHNICAL SUPPORT

If you need assistance in using Quick Heal Firewall Pro, visit its support pages at http://www.quickheal.co.in/public/support/contact_callcentre.asp page for available support options including FAQ, Documentation, Forum, Tips-n-tricks and Troubleshooting.