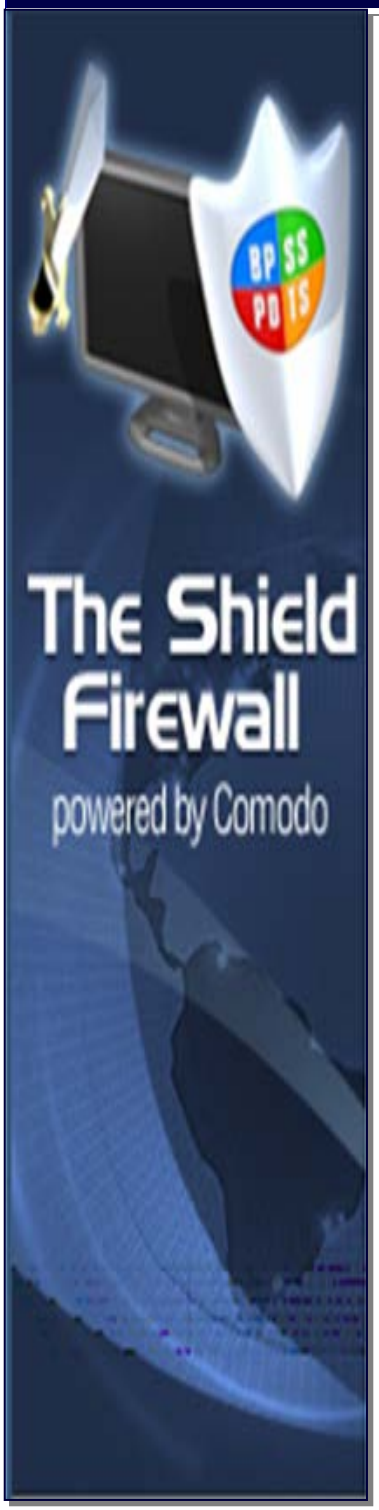
PCSecurityShield

Simple, Affordable Internet Security



Shield Firewall

Powered by Comodo

User Guide

Rev. Jan 2008

Table of Contents

The Shield Firewall - Introduction

Overview

The Shield Firewall offers 360° protection against internal and external threats by combining enterprise class packet filtering firewall with an advanced host intrusion prevention system. The new-look interface facilitates quick and easy access to all major settings, including the powerful and highly configurable security rules interface.

Built from the ground upwards with our security in mind, this award winning firewall constantly monitors and defends your system from inbound and outbound attacks. Version 3.0 now features a fully fledged Host Intrusion Prevention System called Defense+ to protect your critical operating system files and block viruses and malware before they ever get the chance to install. In fact, Defense+ is so good at blocking malware; you may never need a dedicated anti-virus program ever again.

The new-look firewall features a friendly graphical user interface; highly granular configuration options; easily understood and informative alerts; wizard-based detection of trusted zones and much more. The Shield Firewall delivers enterprise class protection and can be used ‘out of the box’ - so even the most inexperienced users will not have to deal with complex configuration issues after installation.

The Shield Firewall 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.

This introductory section is intended to provide an overview of the basics of The Shield Firewall and should be of interest to all users.

Shield Firewall Installation

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

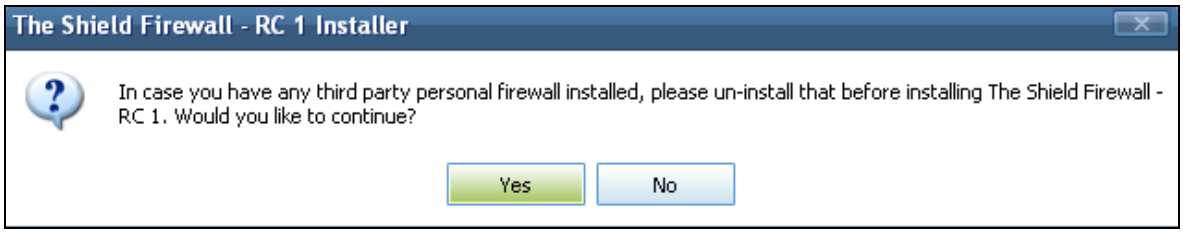
Installation Process

To install, download the Shield Firewall 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

Before you install Shield Firewall, 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 Shield Firewall and reduce the protection offered by it. Click **Yes** to continue.



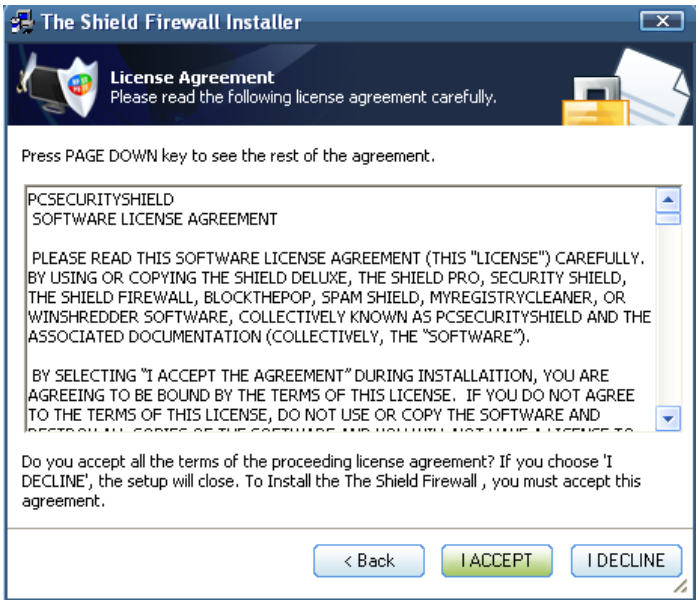
STEP 2: Welcome Dialogue box

The set up program starts automatically and the Welcome wizard is displayed. It is recommended that you exit all Windows programs before running the setup.

- Click '**Next**' to continue.

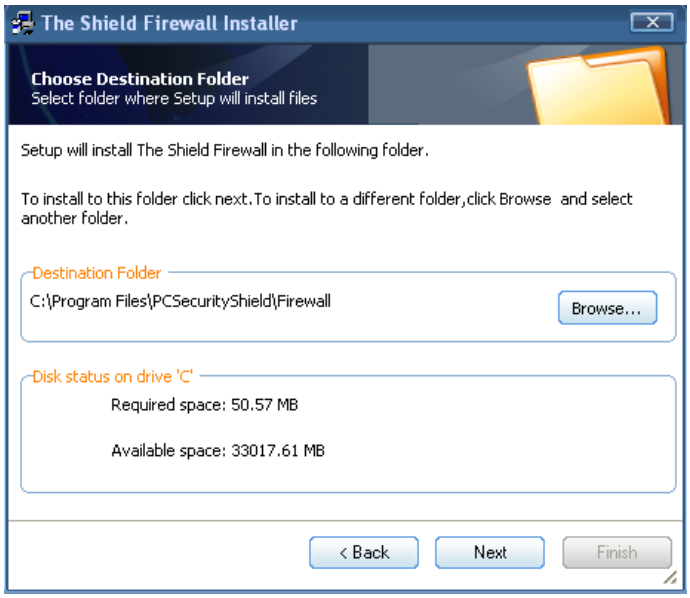
STEP 3: License Agreement

- Read the End-User License Agreement.
- Select "***I accept the terms of the Lincense Agreement***".
- Click on "**Next**"..



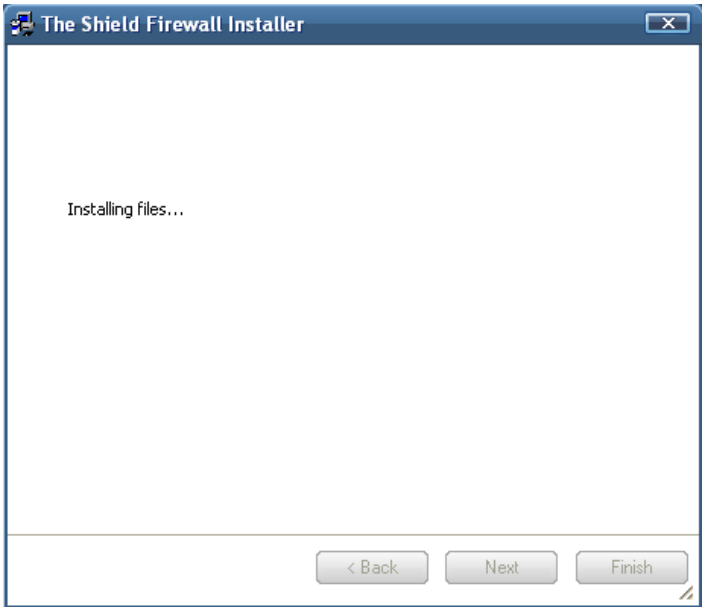
STEP 4: Location Destination Folder

- The **Shield Firewall 2008** application will install in the "**C**" drive. The "**C**" drive is the default setting.
- Click "**Next**" to continue.



STEP 5: Set Up Status Box

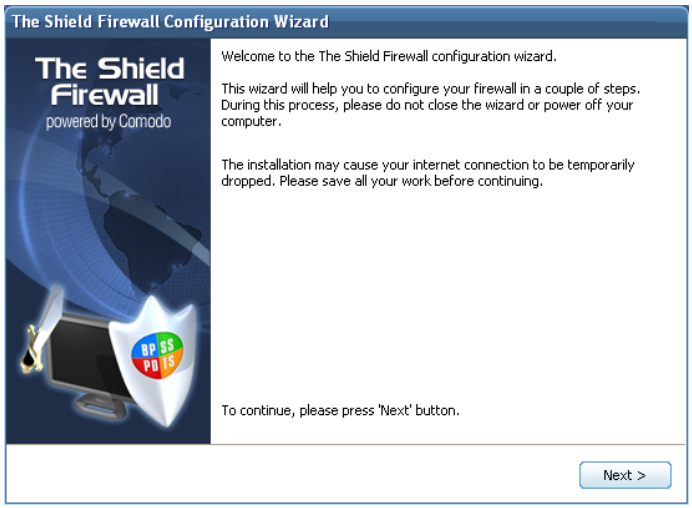
A setup status dialogue box is displayed. You will see a progress bar indicating that files are being installed.

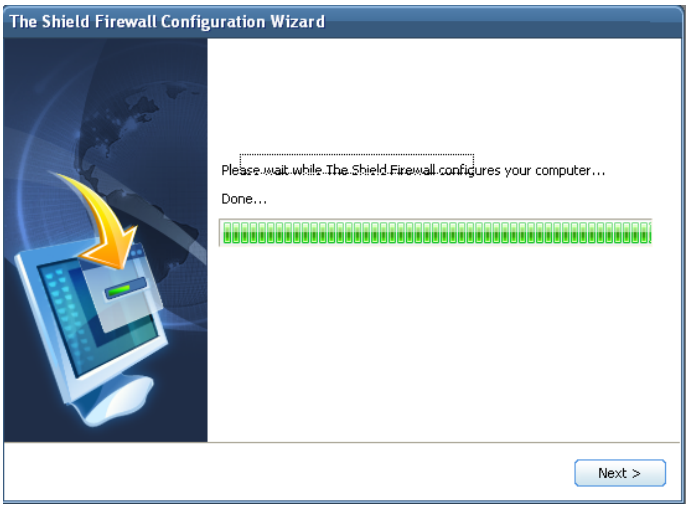


STEP 6: License Configuration

This screen appears only when license is not already activated. It does implicit activation and in that process generates a unique id that it sends to a SHIELD FIREWALL server. If you wish to sign up for

News letter and want to give your email id, you can enter that here. To receive news about Shield Firewall products check the box stating "Sign me up for news about SHIELD FIREWALL products", if you don't wish to receive any news from SHIELD FIREWALL uncheck the box.



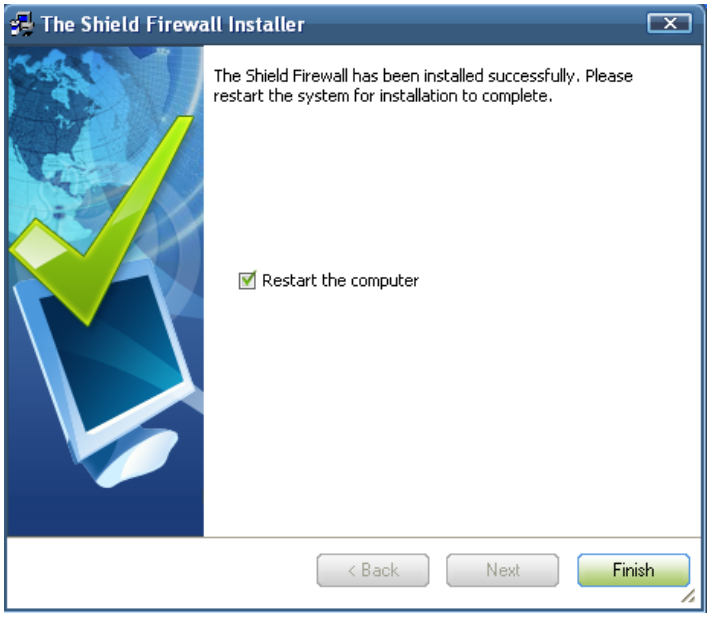


STEP 7: Configuration

- We recommend "***Basic***" mode.
- Click "***Next***".

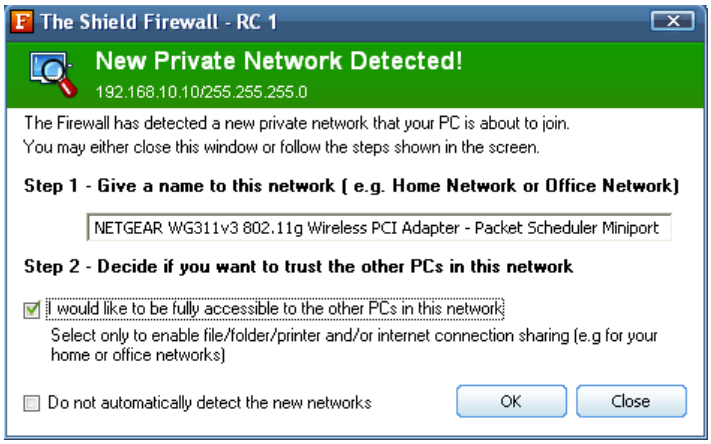
STEP 8: Restart your system

- Restart your computer to complete installation.
- Click "**Finish**".



- **STEP 9: After Installation**

- Post installation the software detects the connection type and automatically adjusts the settings to suite the machine

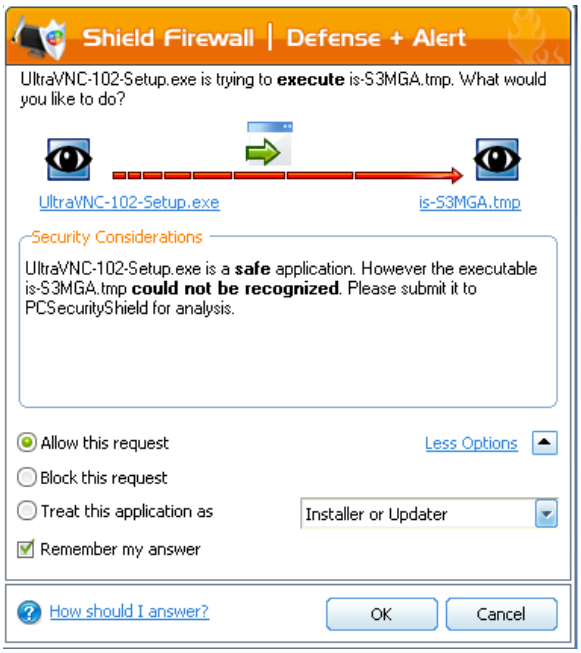


The Shield Firewall icon will be displayed in the System Tray and on the Desktop. To start the Shield Firewall program, double-click on either icon to launch the interface.

Your computer is automatically protected by The Shield firewall every time you start the machine. You do not have to explicitly start The Shield firewall to protect your computer. To completely shut the program down; right-click on The Shield Firewall icon in the System Tray and select 'Exit'. After selecting “Exit”, a dialogue will pop-up confirming your actions. If you select ‘YES’, the Firewall will be disabled and will no longer be protecting your PC.

In addition, as the software gather information about the machine and the allowed application it generates a warning that displays the “Application:” and offers option such as “Allow this request”, block this request Treat this application as (there is a drop down menu; there to select from: Trusted application, Web browser, Email client. Etc) and “Remember my answer”.

** Note that an icon of the software is displayed in addition with the recommend action(s) to apply. **



Starting the Shield Firewall

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

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

1. The Shield Firewall Tray Icon

Just double click the shield icon to start the main firewall interface. (By right-clicking on the tray icon, you can access short cuts to other firewall settings)

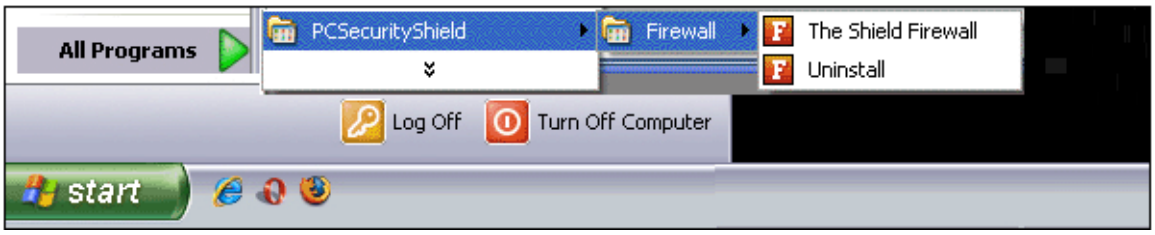
2. Windows Desktop

Just double click the shield icon in the desktop to start The Shield Firewall .

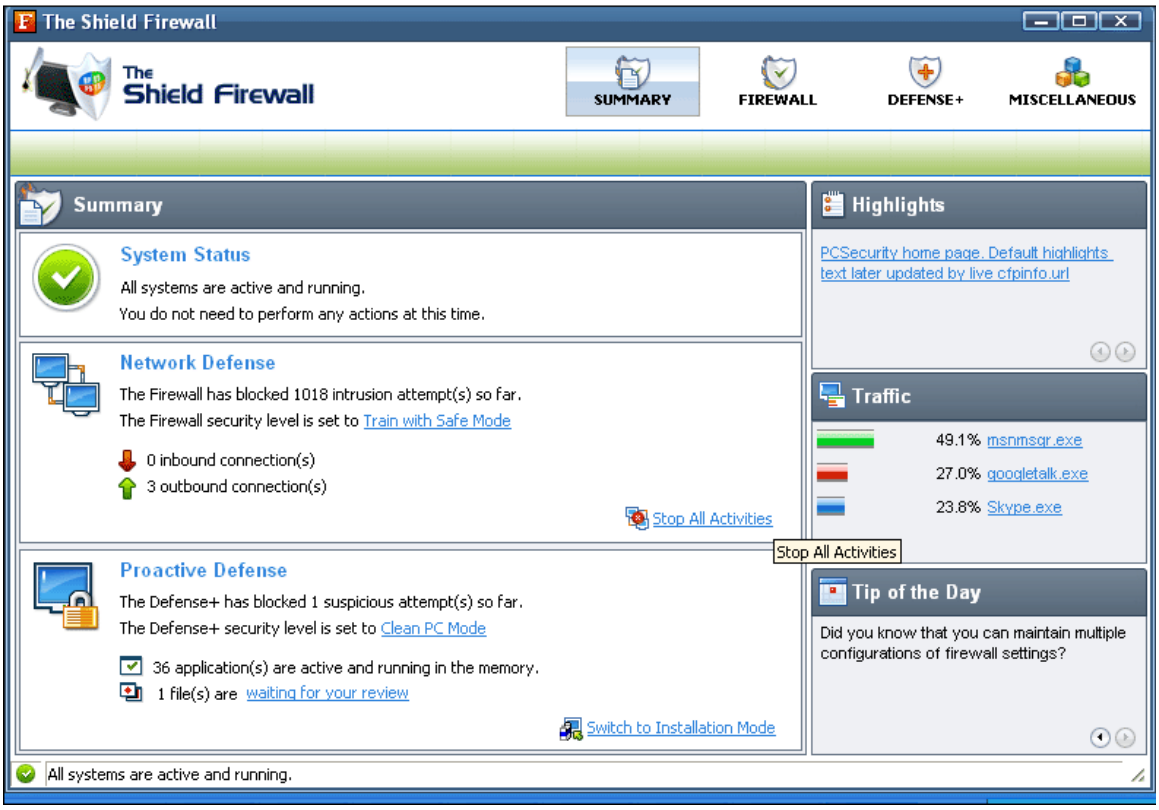
3. Start Menu

You can also access The Shield Firewall via the Windows Start Menu.

Click 'Start' and select All Programs->The Shield-> Firewall->The Shield Firewall.



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


The Shield Firewall
The Shield Firewall
SUMMARY
FIREWALL
DEFENSE+
MISCELLANEOUS
Summary
System Status
All systems are active and running.
You do not need to perform any actions at this time.
Network Defense
The Firewall has blocked 1018 intrusion attempt(s) so far.
The Firewall security level is set to Train with Safe Mode
0 inbound connection(s)
3 outbound connection(s)
Stop All Activities
Proactive Defense
The Defense+ has blocked 1 suspicious attempt(s) so far.
The Defense+ security level is set to Clean PC Mode
36 application(s) are active and running in the memory.
1 file(s) are waiting for your review
Switch to Installation Mode
Highlights
PCSecurity home page. Default highlights text later updated by live cfpinfo.url
Traffic
49.1% msnmsgr.exe
27.0% googletalk.exe
23.8% Skype.exe
Stop All Activities
Tip of the Day
Did you know that you can maintain multiple configurations of firewall settings?
All systems are active and running.

The Shield Firewall - Navigation

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

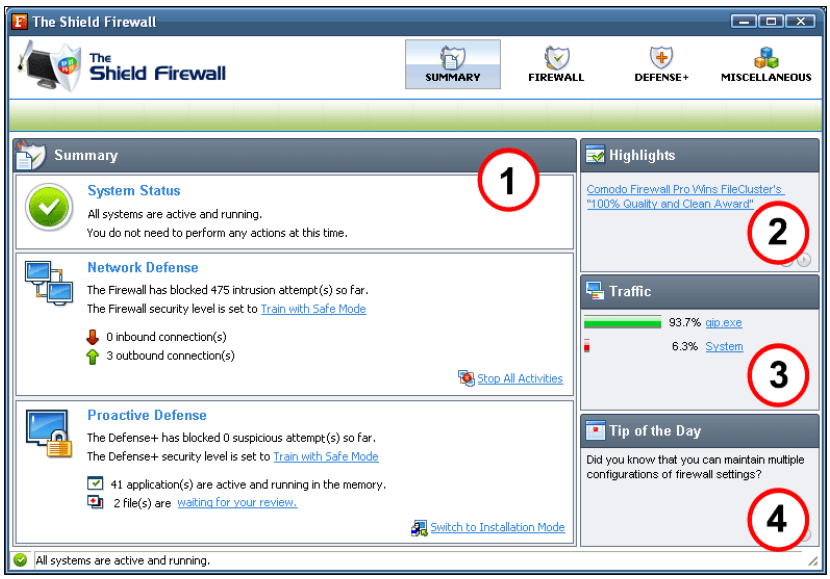
The Shield Firewall is divided into four main areas indicated by the icons at the top right hand corner of the interface. Each of these areas contains several sub-sections that allow you total control over configuration of the firewall and defense+ settings.

- **Summary** - contains at-a-glance details of firewall settings, activity and new.
- **Firewall** - clicking this icon will take you to the 'Firewall Tasks' configuration area. Advanced users are advised to first visit the Network Security Policy area for an introduction to firewall policies and rule creation
- **Defense+** - clicking this icon will take you to the 'Defense+' configuration area. Advanced users are advised to first visit the Computer Security Policy area for an introduction to Defense+ policies and rule creation
- **Miscellaneous** - clicking this icon will take you to the 'Miscellaneous' options section which contains several areas relating to overall configuration.

The icon nav-bar is ever-present and can be accessed at all times.

Firewall Summary

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



1. **Summary** :

    - **System Status** - shows systems activity and recommendations on actions you need to perform.

    - **Network Defense** - The Shield Firewall allows you to customize firewall security by using the Firewall Security Level slider to move between preset security levels. This section also allows you to configure the frequency of alerts. The current security level (or 'Firewall Behavior Setting) is shown in blue, underlined font - 'Learn Safe Only' is the Firewall security setting in the example shown above. Clicking on this blue text opens the firewall behavior panel and allows you to adjust the security level to your own preferences. For a complete explanation of this part of the firewall, please see 'Firewall Behavior Settings'.

    - **Proactive Defense** - The Shield Firewall allows you to customize Defense+ security by using the Computer Security Level slider to move between preset security levels. This section also allows you to configure which processes are monitored by the Defense+ module. The current Defense+ security level is shown in blue, underlined font - 'Learn Safe Only' is the Firewall security setting in the example shown above. Clicking on this blue text opens the Defense+ configuration panel and allows you to configure the security level to your own preferences. For a complete explanation of this section, please see 'Defense+ Settings'.

2. **Highlights** - The Highlights section displays information about Security Alerts and News related to The Shield Firewall & latest Critical security updates. Clicking on the text in the Highlights box takes you to the Shield website to read more details.

3. **Traffic -** The summary screen of The Shield Firewall displays a bar graph showing the applications that are currently connected to the internet and are sending or receiving data. The summary also displays the % of total traffic each application is responsible for and the filename of the executable. Clicking on any application leads to the more detailed 'View Active Connections' interface.

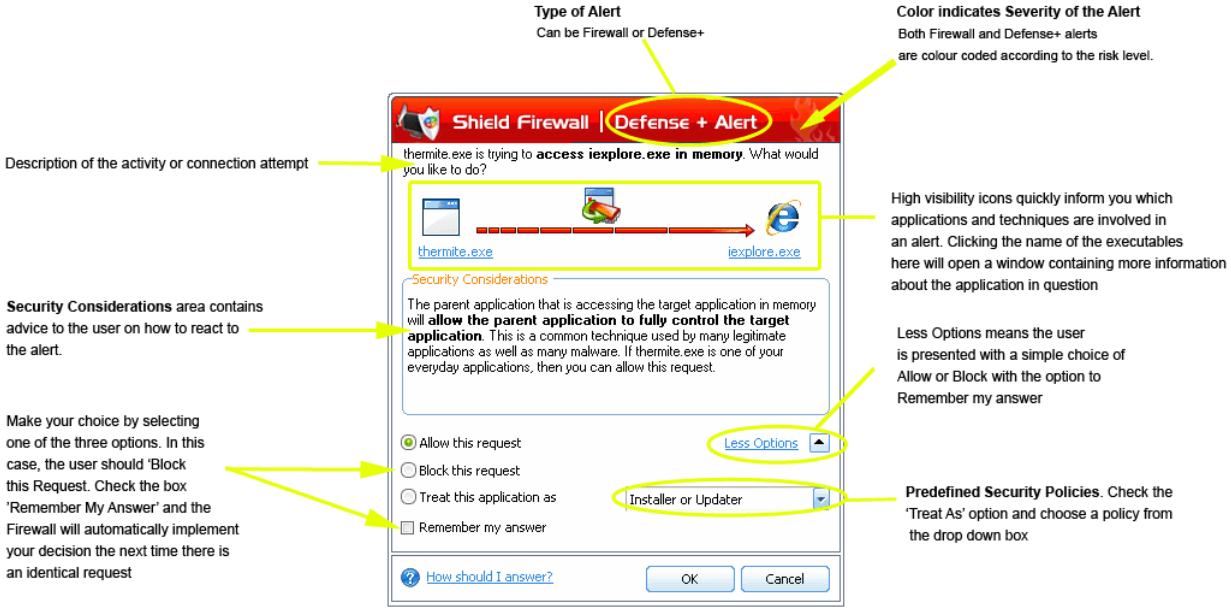
4. **Tip of the Day -** This section contains helps you to use The Shield Firewall to its maximum potential by displaying information about features you may have missed.

Understanding Alerts

After first installing The Shield Firewall , it is likely that you will see a number of pop-up alerts. This is perfectly normal and indicates that the firewall is learning your the behavior of your applications and establishing which programs need internet access. Each alert provides information and options to allow or block any request and to instruct the firewall how to behave in future.

Alerts Overview

The Shield Firewall alerts come in two varieties, Firewall Alerts and Defense+ Alerts. Broadly speaking, Firewall alerts inform you about network connection attempts, whereas Defense+ alerts tell you about the behavior of application on your system. In both cases, the alert can contain very important security warnings or may simply occur because you are running an application for the first time. Your reaction should depend on the information that is presented at the alert.



Red Alerts - High Severity - These alerts indicate highly suspicious behavior that is consistent with the activity of a Trojan horse, virus or other malware program. Carefully read the information provided when deciding whether to allow it to proceed.

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

How Should I answer the Firewall Alerts?

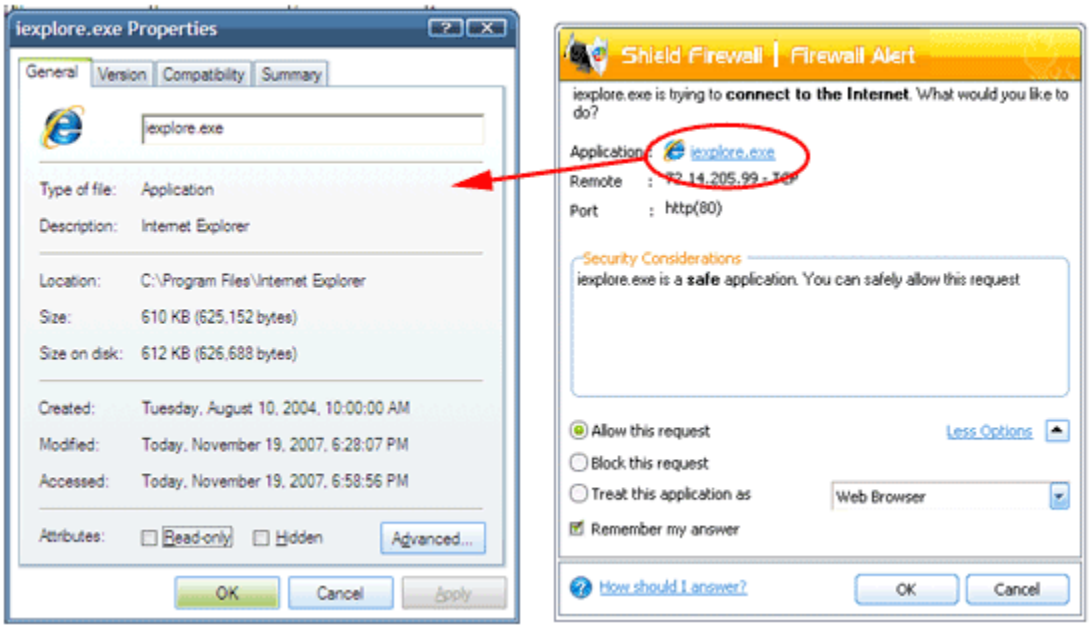
Points to consider:

1. Carefully read the 'Security Considerations' section. The Shield Firewall can recognize thousands of safe applications. (For example, Internet Explorer and Outlook are safe applications). If the application is known to be safe - it is written directly in the security considerations section along with advice that it is safe to proceed. Similarly, if the application

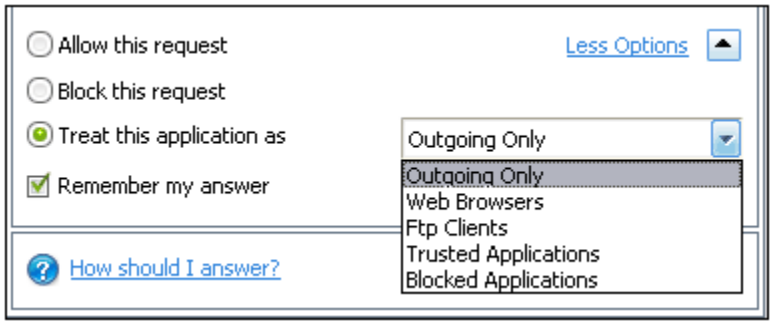
is unknown and cannot be recognized you will be informed of this. If it is one of your everyday applications that you want to grant internet access to then you should 'Allow This Request' (it may be the case that the application has not yet been added to the safe application database yet).

If you don't recognize the application then we recommend you select 'Block This Request' but don't select the 'Remember My Answer' checkbox.

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



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



If you do not see the 'Treat this Application As' option, you should click 'More Options'. Remember to check the box 'Remember My Answer'.

3. If The Shield Firewall reports behavior consistent with that of malware in the security considerations section then you should block the request AND click 'Remember My Answer' to make the setting permanent.

How Should I answer the Defense+I Alerts?

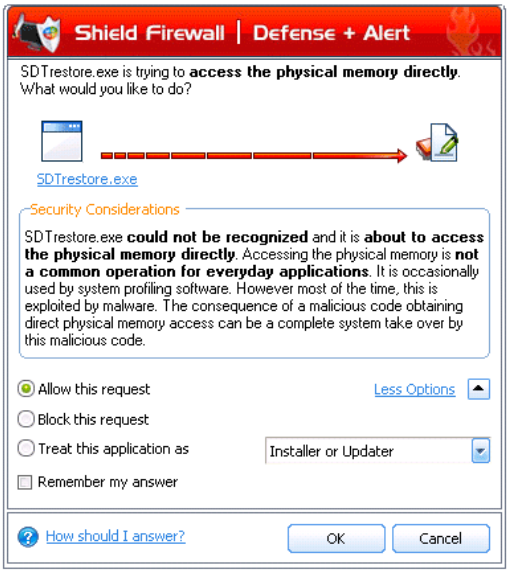
Points to consider:

1. As with Firewall Alerts, carefully read the 'Security Considerations' section. The Shield Firewall can recognize thousands of safe applications. If the application is known to be safe - it is written directly in the security considerations section along with advice that it is safe to proceed. Similarly, if the application is unknown and cannot be recognized you will be informed of this. If it is one of your everyday applications that you want to grant execution rights to then you should 'Allow This Request'. If you don't recognize the application then we recommend you select 'Block This Request' but don't select the 'Remember My Answer' checkbox.

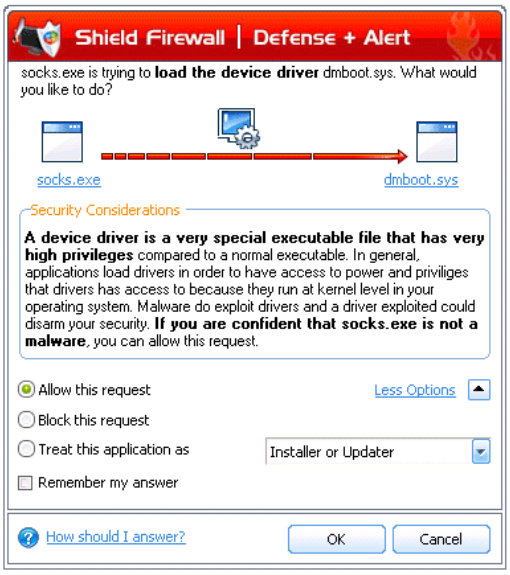
If you don't recognize the application then we recommend you select 'Block This Request' but don't select the 'Remember My Answer' checkbox.

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

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

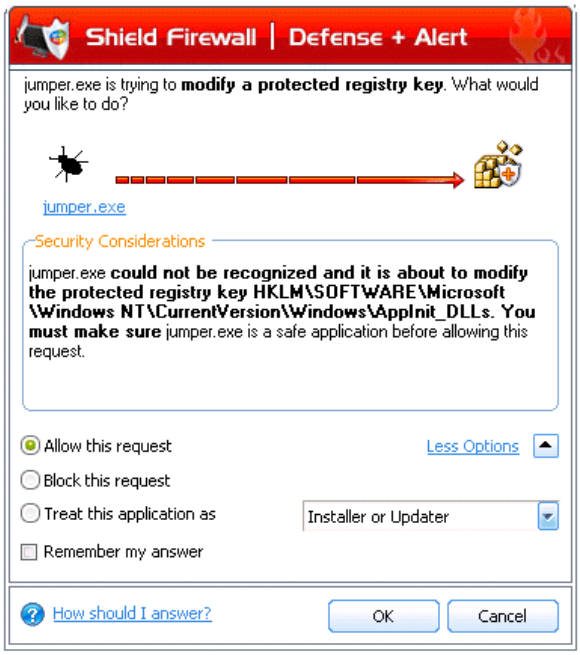


Physical Memory Access Alert



Device Driver Installation Alert

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

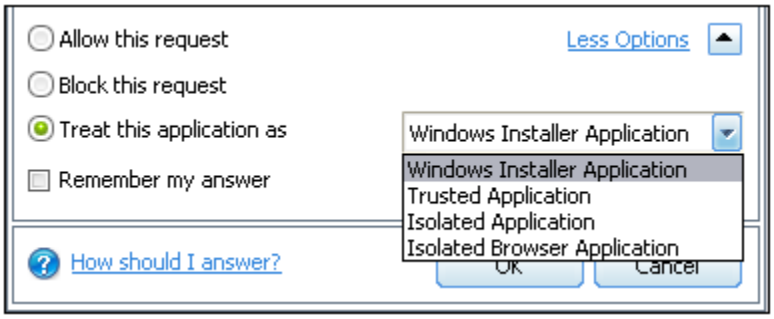


Protected Registry Key Alert

5. 'Protected File Alerts' usually when you try to download, copy files or when you update an already installed application. Were you installing new software or trying to download an application from the internet? If you are downloading a file from the Internet, try to use the 'Allow without Remembering' option to cut down on the creation of unnecessary rules within the firewall.

If an application is trying to create an executable file in the Windows directory (or any of its subdirectories) then pays special attention. The Windows directory is a favorite target of malware applications. If you are not installing any new applications or updating Windows then make sure you recognize the application in question. If 'Block This Request' without checking the 'Remember My Answer' box.

If an application is trying to create a new file with a random filename e.g. "hughbasd.dll" then it is probably a virus and you should block it permanently by selecting 'Treat As' 'Isolated Application' (third down in the graphic below)



6. If The Shield Firewall reports a malware behavior in the security considerations section then you should block the request permanently by also selecting the 'Remember My Answer' option. As this is probably a virus, you should also sumbit the application in question to The Shield for analysis.

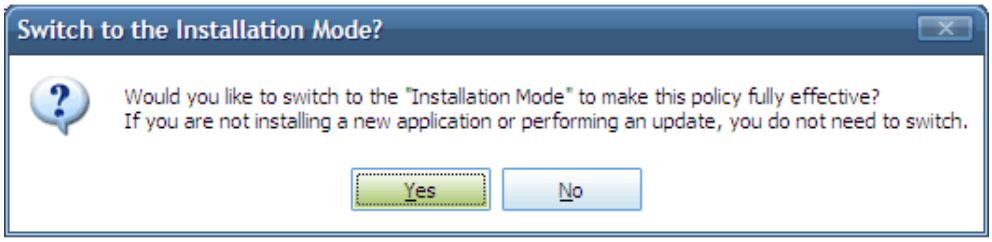
7. Unrecognized applications are not always bad. Your best loved applications may very well be safe but not yet included in the PCSecurity certified application database. If the security considerations section says “If xxx is one of your everyday applications, you can allow this request”, you may allow the request permanently if you are sure it is not a virus. You may report it to PCSecurity for further analysis and inclusion in the certified application database.

8. If Defense+ is in Clean PC Mode, you will probably be seeing the alerts for any new applications introduced to the system - but not for the ones you have already installed. You may review the 'My Pending Files' section for your newly installed applications and remove them from the list for them to be considered as clean.

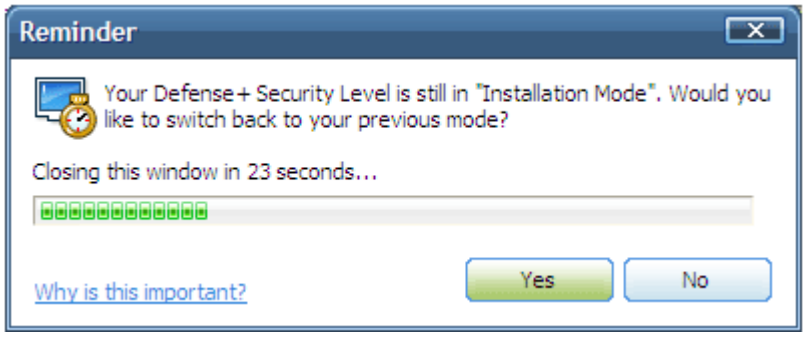
9. Avoid using “Trusted Application” or “Windows System Application” policies for you email clients, web browsers, IM or P2P applications. These applications do not need such powerful access rights.

10. In 'Paranoid Mode', 'Train with Safe Mode' and 'Clean PC' mode, The Shield Firewall will make it easy to install new applications that you trust by offering you the opportunity to temporarily engage 'Installation Mode'. If installing new unknown application.

Defense+ will alert you with a pop-up notification and, as you want to allow this application to continue installing, you should select 'Treat this application as an Installer or Updater'. You will subsequently see the following:



This will be followed by the following reminder:



Firewall Task Center

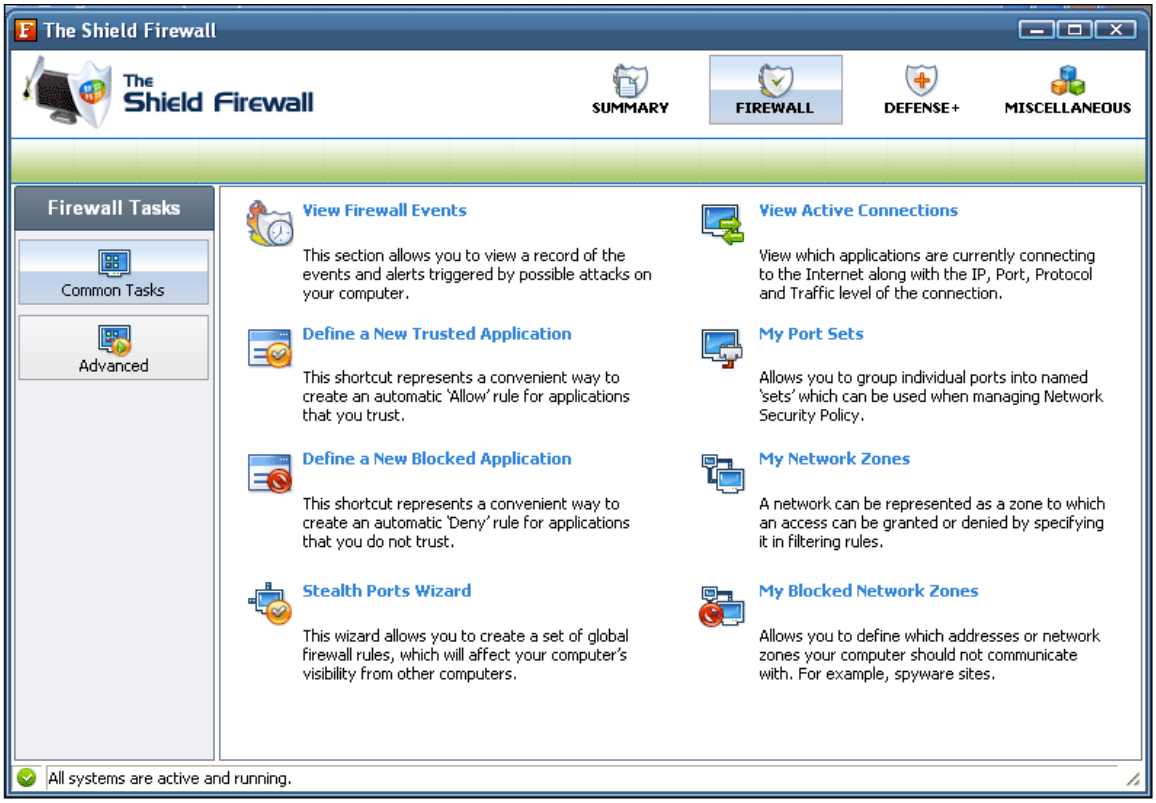
The Firewall Task Center allows you to quickly and easily configure all aspects of the Firewall and divided into two sections: Common Tasks and Advanced Tasks

It can be accessed at all times by clicking on the Firewall Shield button. (third button from the top right)

Common Tasks

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

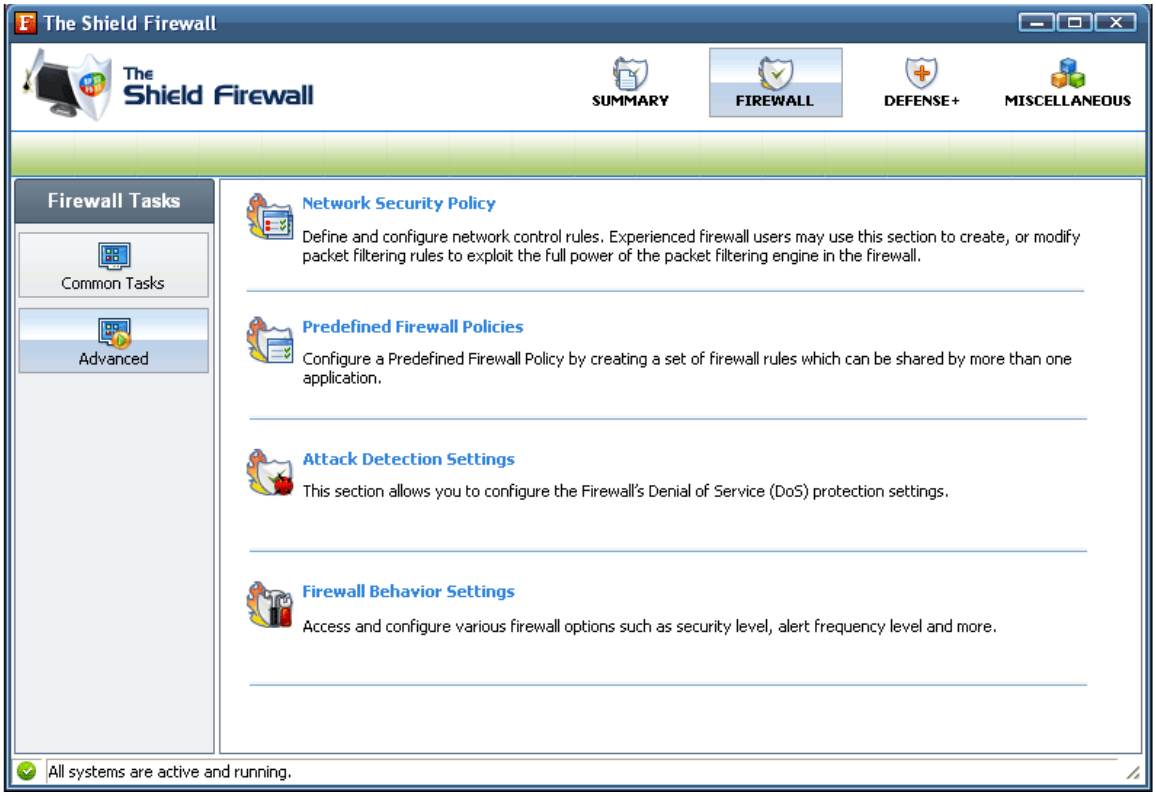
- View Firewall Events
- Define a New Trusted Application
- Define a New Blocked Application
- Stealth Ports Wizard
- View Active Connections
- My Port Sets
- My Network Zones
- My Blocked Network Zones



Advanced Tasks

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

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



Defense+ Tasks Overview

The Defense+ component of The Shield Firewall is a host intrusion prevention system that constantly monitors the activities of all executable files on your PC. With Defense+ activated, the user is warned EVERY time an unknown application executable (.exe, .dll, .sys, .bat etc) attempts to run. The only executables that are allowed to run are the ones you give permission to.

The Defense+ Task Center allows you to quickly and easily configure all aspects of Defense+ and is divided into two sections: Common tasks and Advanced.

It can be accessed at all times by clicking on the Defense+ Shield button (second button from the top right)

Common Tasks

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

- View Defense+ Events
- My Protected Files
- My Quarantined Files
- My Pending Files
- My Own Safe Files
- View Active Process List
- My Trusted Software Vendors
- My Protected Registry Keys
- My Protected COM Interfaces

Advanced

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

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

Miscellaneous Overview

The 'Miscellaneous' section contains several areas relating to overall configuration as well as handy utilities and shortcuts to help enhance and improve your firewall experience.

You have the following options to choose from:

- Settings: Allows the user to configure general firewall settings (password protection, update options, language, theme etc.)
- Manage My Configurations: Allows the user to manage, import and export their firewall configuration profile
- Diagnostics: Helps identify any problems with your installation
- Check For Updates: Launches The Shield Firewall updater
- Submit Suspicious Files: Allows users to send suspicious files to PCSecurityShield for analysis and possible inclusion on the PCSecurityShield safelist.
- Browse Support Forums: Link to rethe Shield User Forums.
- Help: Launches this help guide
- About: Displays version and copy-right information about the product.