



OUTPOSTPRO

FIREWALL

Getting Started

Abstract

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

Table of contents

1 Installing and registering Outpost Firewall	4
1.1 System Requirements	4
1.2 Installing Outpost Firewall Pro	4
1.3 Registering Outpost Firewall Pro	11
2 User Interface and Controls Basics	12
2.1 The Toolbar	14
2.2 Left and Information Panels.....	14
2.3 System Tray Icon.....	16
2.4 Interface Language	18
3 Basic Configuration	18
3.1 Starting and Stopping Protection.....	19
3.2 Managing Protection Status	21
3.2 Selecting the Firewall Policy	22
3.2.1 Running in Rules Wizard Mode.....	24
3.2.2 Smart Advisor	25
3.3 Running in Auto-Learn Mode	26
3.4 Running in Entertainment Mode.....	26
3.5 Protecting Configuration with a Password	27
4 Updating Outpost Firewall Pro	29
4.1 Configuring Updates.....	29
4.2 Agnitum ImproveNet.....	31
5 Performing a System Scan	32
5.1 Selecting Scan Type	32
5.2 Scanning Specified Locations	33
5.3 Removing Detected Malware	33
5.4 Viewing Scan Results	34
6 Uninstalling Outpost Firewall Pro	36
7 Troubleshooting	37
About Agnitum	38

1 Installing and registering Outpost Firewall

1.1 System Requirements

Outpost Firewall Pro can be installed on Windows 2000 SP4, Windows XP, Windows Server 2003, Windows Vista, or Windows 7 operating systems. The minimum system requirements for Outpost Firewall Pro are:

- CPU: 450 MHz Intel Pentium or compatible;
- Memory: 256 MB;
- Hard disk space: 100 MB.

Note:

- Outpost Firewall Pro is available both for 32-bit and 64-bit versions of operating systems. Please download the corresponding version from Agnitum's web site: www.agnitum.com.
- No special network adapter or modem and no special network configuration settings are needed for the normal operation of the software.
- Outpost Firewall Pro should not be run with any other security software. Running Outpost Firewall Pro with other security products can result in system instability (i.e. crashes) and can cause your system to operate in an insecure mode.

1.2 Installing Outpost Firewall Pro

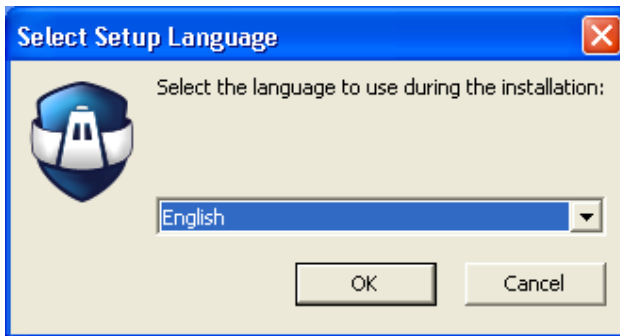
Outpost Firewall Pro's installation procedure is similar to that of most Windows programs.

To start the installation program of the Outpost Firewall Pro system:

1. **Very Important!** Before installing Outpost Firewall Pro, uninstall any other firewall software on your computer and reboot.
2. Close all open applications.
 - a) if you install the product downloaded from the site, click OutpostFirewallProInstall.exe;
3. b) if you install the product from a disk, setup wizard should run automatically. If automatic running failed, click the **Start** button on the Windows task bar and select **Run**. In the **Open** field of the **Run** dialog window, enter the full path to the setup program file (OutpostFirewallProInstall.exe). For example, if the setup program is on disk D: in the folder Downloads and subfolder Outpost, type into this field:
D:\downloads\outpost\OutpostFirewallProInstall.exe
4. Click the **OK** button.

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 wizard and aborts the entire setup procedure.

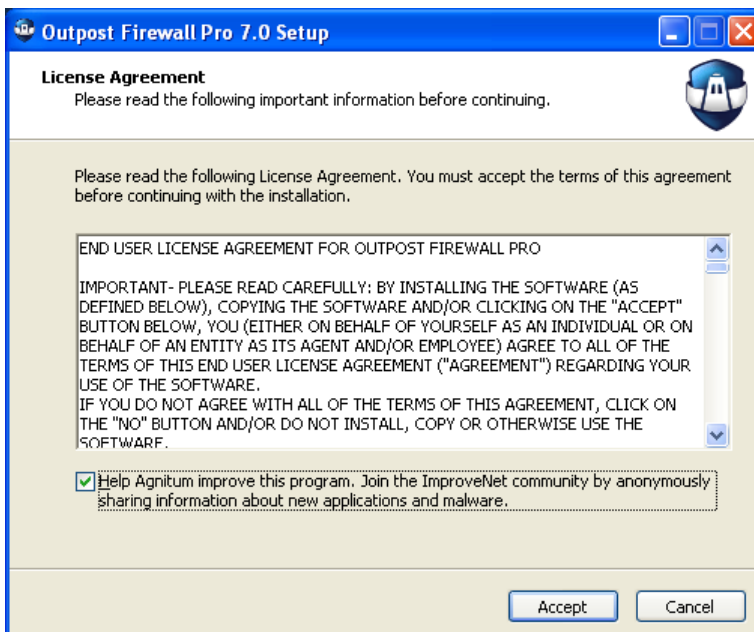
The installation begins with **Select Language** dialog.



Choose the language for Outpost Firewall Pro interface and click **OK**. Setup will display the **Welcome** dialog presenting basic features of the product:



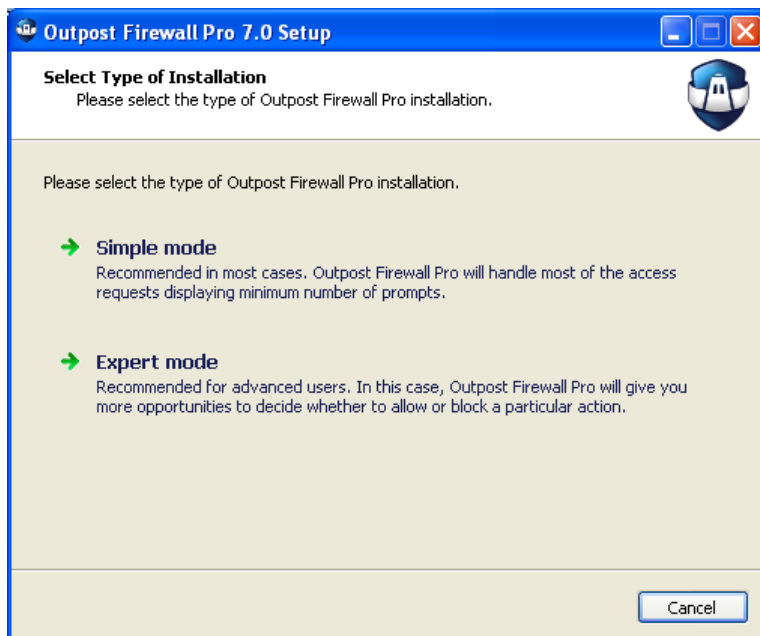
After clicking the **Next** button you will be asked to accept the License Agreement to use the **Outpost Firewall Pro**. Please read it carefully.



At this step, you can also join Agnitum's ImproveNet program to help improve the quality, security and control features of Agnitum products by selecting the **Help Agnitum improve this program** check box.

Click **Accept** to proceed.

The setup wizard will offer you to select a type of installation:

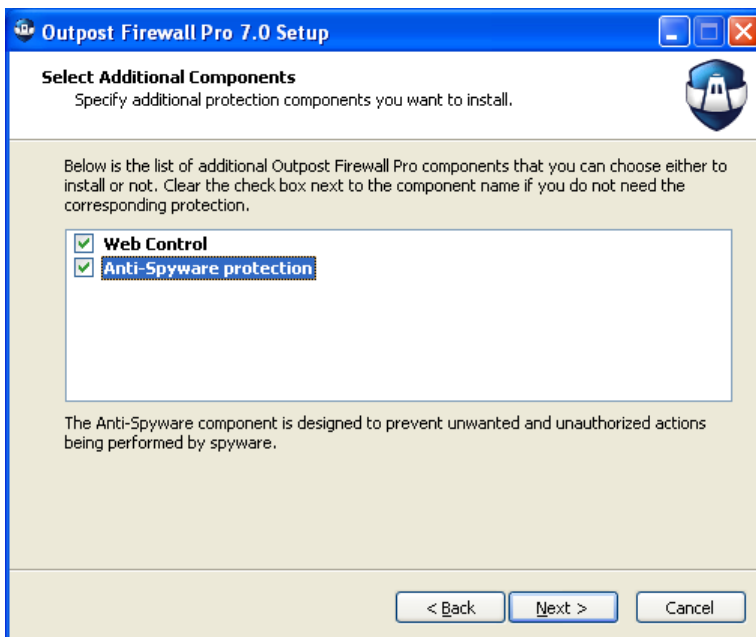


Simple mode provides a reduced number of product prompts that require your response and is recommended for most cases. **Expert** mode gives you more opportunities to decide whether to allow or block a particular access request and is recommended for advanced users.

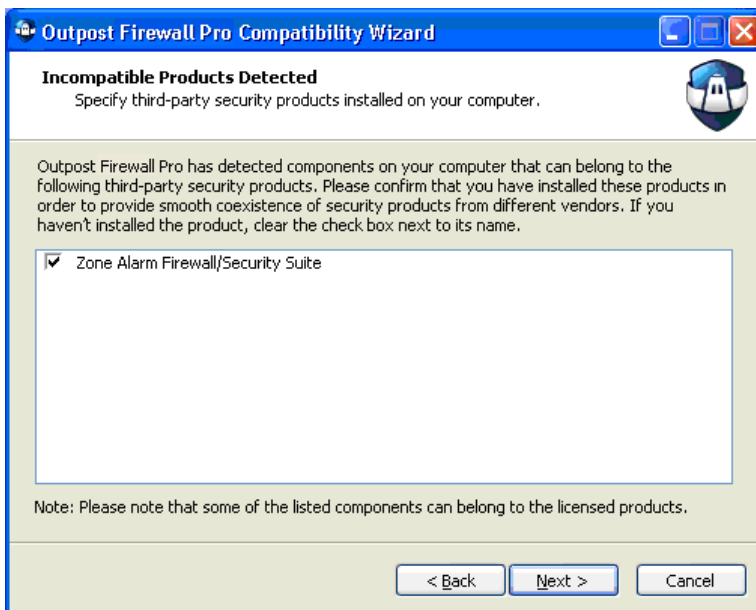
Note:

- Depending on the selected installation type Outpost Firewall Pro main window will get its interface view—**Simple View** in the case of **Simple** mode and **Expert View** in the case of **Expert** mode.

Click the desired operation mode to proceed. If you have selected the **Expert** mode, the setup wizard will allow you to specify a few settings more. The next step allows to choose product components to install on the computer. Select the corresponding check boxes and click **Next**.



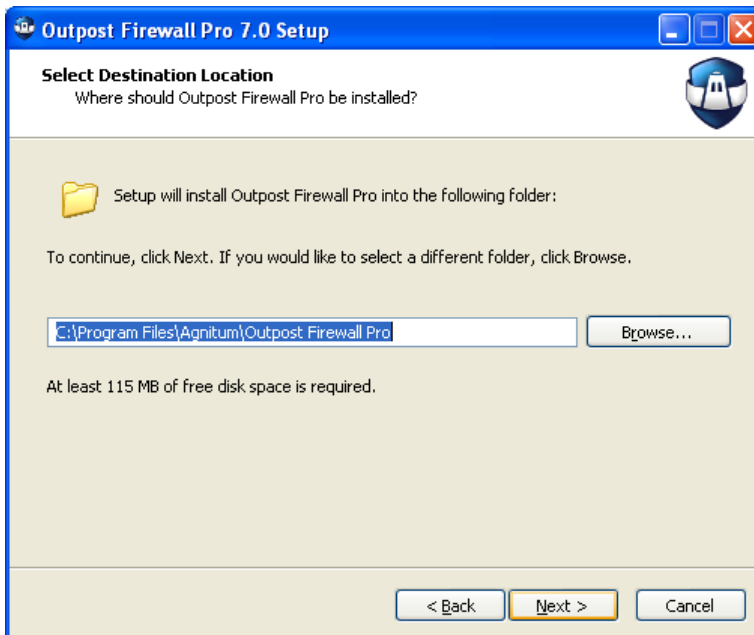
In case you have not removed any third-party security software, the setup wizard will display a prompt pointing at detecting incompatible software:



On detecting *an incompatible product* on your system the setup wizard will be unable to continue further installation until you remove the product.

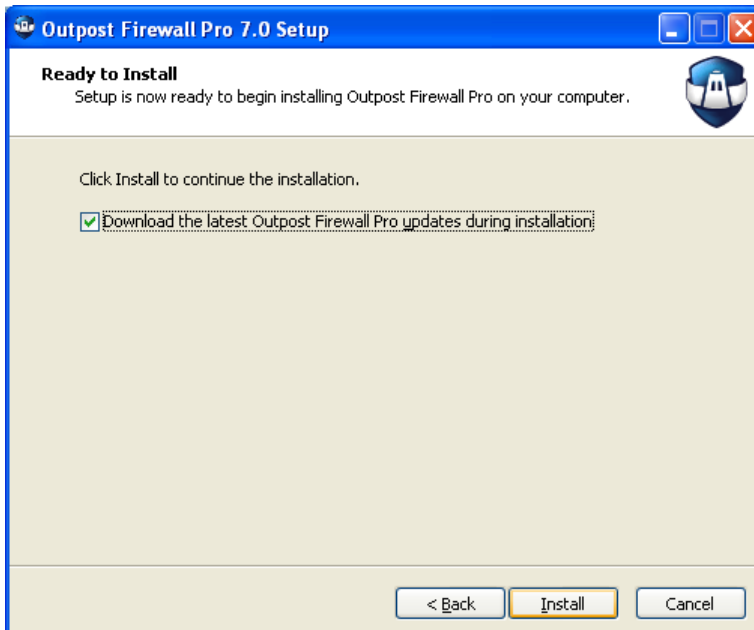
On detecting *a partly compatible product* the wizard will offer you one of the possible options to apply to the product.

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



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

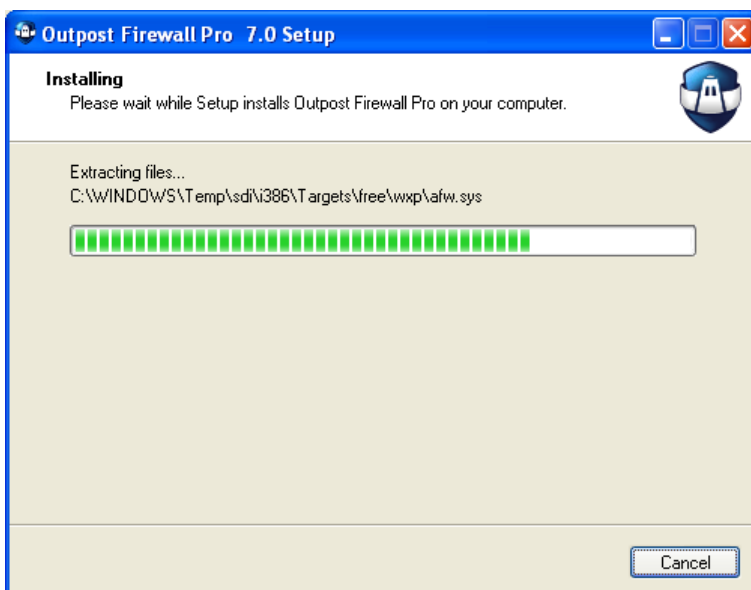
If you want to change the default file location, click **Browse**. Select the folder or create your own one and click **OK**. Click **Next** to proceed to the last step before actual installation:



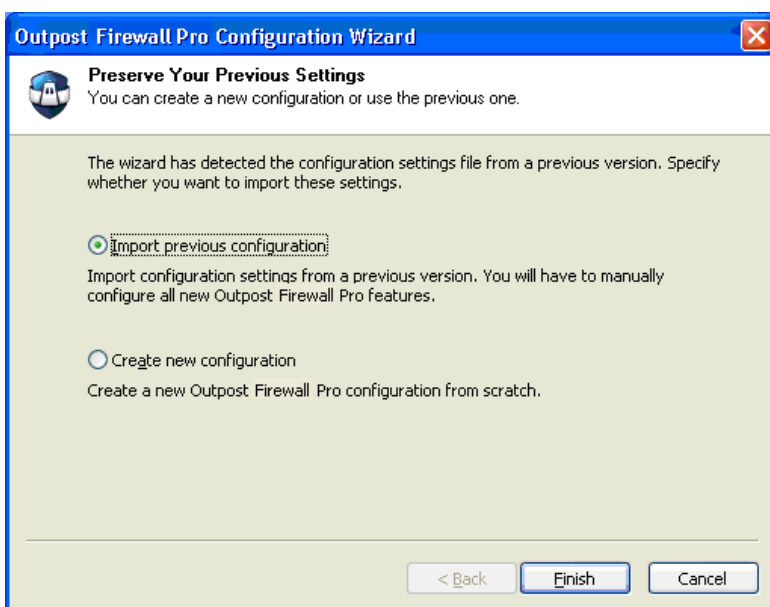
Select the **Download the latest Outpost Firewall Pro updates during installation** option to download rules presets for the product.

This is the final step before starting the installation process. 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:

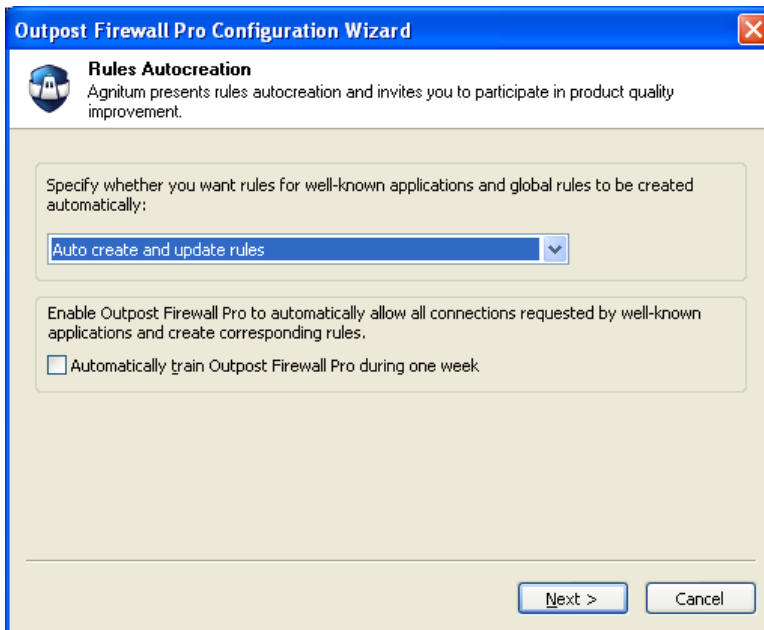


After the installation is finished, the **Configuration Wizard** will help you create a new configuration or import the previous if you install the product over an earlier version:



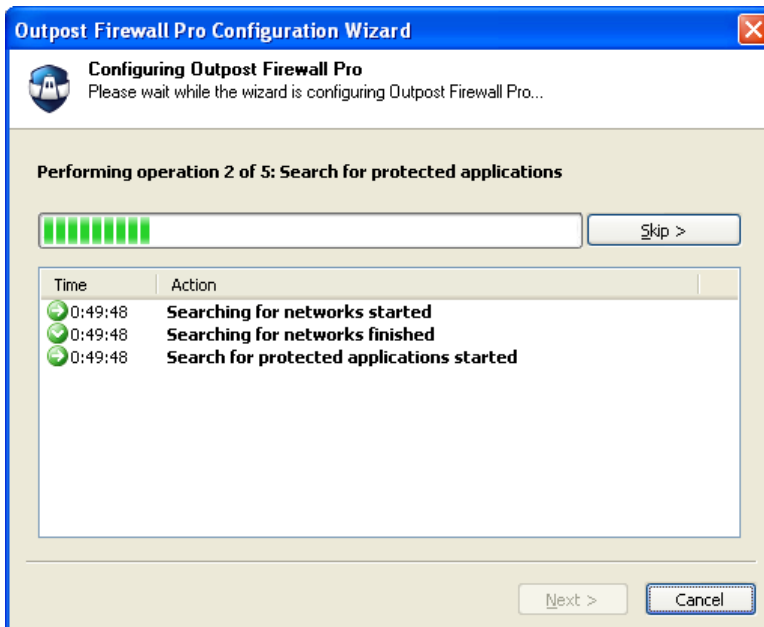
On importing a previous configuration the system will automatically copy saved settings of the earlier version, after which you will need to reboot the computer to complete Outpost Firewall Pro installation.

On creating a new configuration the setup wizard will proceed to the **Rules Autocreation** step, which lets you to enable rules autocreation, so global rules and rules for well-known applications are created automatically when they first request an action (for example, network access or process memory modification). If you do not want to enable rules autocreation, select **Use predefined rules** for the rule sets to be created according to our engineers' built-in presets in order to provide optimal system performance and application security:



The **Automatically train Outpost Firewall Pro during one week** option allows product to create necessary rules automatically.

After clicking **Next**, Outpost 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 selected 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:



Important:

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

1.3 Registering Outpost Firewall Pro

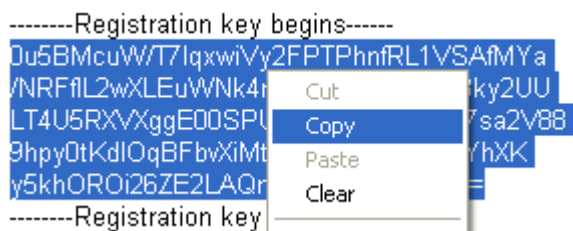
Outpost Firewall Pro is available for your free evaluation. You are entitled to evaluate the software during the trial period with no obligation to pay. After the trial period, if you decide to keep the software and would like to receive free annual updates, you must register your copy with us for a small fee.

If you bought Outpost Firewall Pro in a box from a store, please follow the instructions on the registration card.

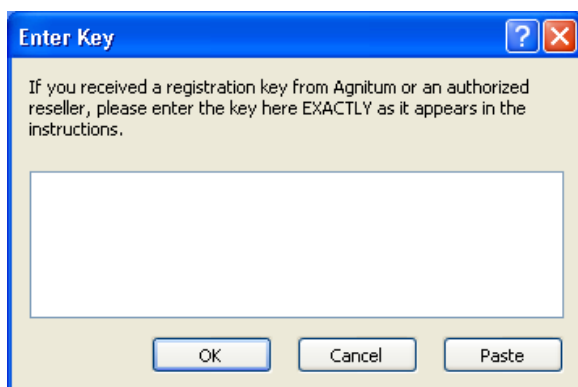
If you downloaded your copy from Agnitum's web site, to register your version, you need to purchase your registration key. Follow the instructions on the page <http://www.agnitum.com/purchase/outpost/> and you will receive your registration key by e-mail.

How to enter your registration key

1. When you receive your registration key, open the e-mail message that contains it and select all the text between **Registration key begins** and **Registration key ends** using your mouse (left-click just before the first character in the first line of the key and while holding down the left mouse button move the mouse just past the last character in the last string of the key, release the mouse button when you have highlighted the entire key as shown in the picture below).
2. Right-click anywhere inside the highlighted text (from step 1) and select **Copy** from the shortcut menu to copy your registration key to the Clipboard (a generally invisible area of Windows used for Copy and Paste actions).



3. Select **Start > Programs > Agnitum > Outpost Firewall Pro** and click **Enter Registration Key**. In the **Enter Key** window, click the **Paste** button and your registration key (which you copied to the Clipboard in step 2) will be inserted into the blank box from the Clipboard:



4. Click **OK** to save your key and close the dialog.

When you buy an Outpost Firewall Pro license, you actually get two licenses:

- A license for Outpost Firewall Pro usage (lifelong);
- A license for free upgrades and support for one year (including the latest Outpost Firewall Pro versions).

In a year you can either buy a renewal license for another year of upgrades and support (Annual Update and Support contract) or simply continue using your last updated version of Outpost Firewall Pro. To purchase a renewal, visit this page: <http://www.agnitum.com/purchase/renewal/index.php>.

Note:

- Outpost Security Suite Pro and Outpost Firewall Pro are independent products and their registration keys are not interchangeable. It means that Outpost Security Suite Pro registration key is not applicable to Outpost Firewall Pro and visa versa. Please, be sure you are entering the correct registration key.

2 User Interface and Controls Basics

When you launch Outpost Firewall Pro for the first time, its main window is displayed. The main window is your central control panel for the suite. Its purpose is to let you monitor network operations of your computer and to modify product settings.

The main window is very similar to Windows Explorer, so should be familiar to most users making Outpost Firewall Pro quite easy to use.

The main window looks like the following:



To display the main window when it is minimized to the system tray:

1. Right-click the firewall's system tray icon.
2. Select **Show/Hide**.

To close the Outpost Firewall Pro main window, click the X in the right-upper corner. Note that this does not shut down the product; the main window is simply minimized and the suite icon remains in the system tray indicating that it is running and protecting your system.

The main window contains:

- **The toolbar**
- **Left panel**
- **Information panel**
- **Status bar**

The status bar is at the bottom of the main window. It is used to display the Outpost Firewall Pro's current state.

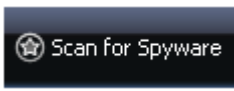
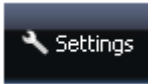

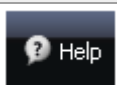
2.1 The Toolbar

The toolbar is close to the top of the main window. To see what each button does, hold your cursor over it for a second. Each button on the toolbar (except the **Settings** button) is a shortcut to one of the product functions. These buttons are simply an easy and direct path to their functions rather than having to go through several different dialog windows to access the same functions.

The toolbar looks like the following:



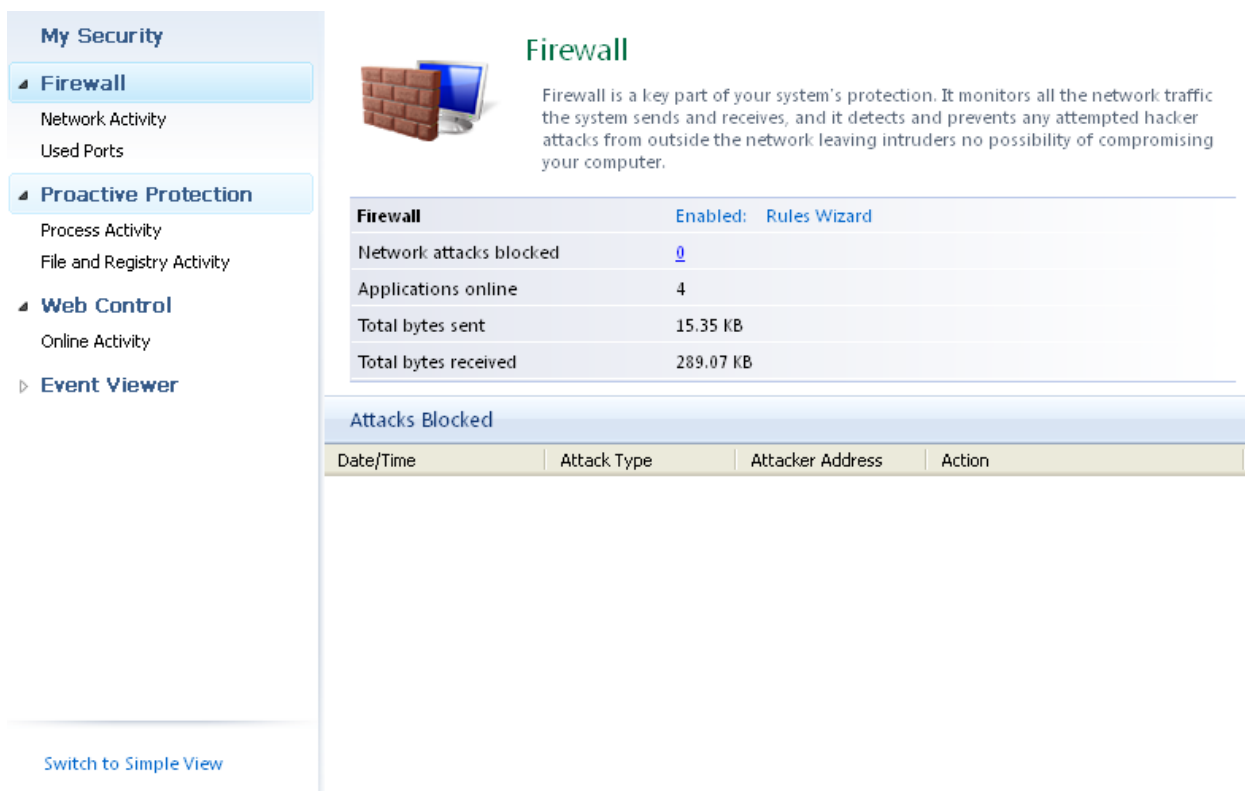
These are the buttons found on the toolbar:

Button	Function
	Starts the malware system scan.
	Opens Outpost Firewall Pro's Settings dialog.
	Downloads the latest product updates including rules presets and anti-malware databases.
	Opens this help file that you are currently reading.

2.2 Left and Information Panels

To display information so you can easily find it, Outpost Firewall Pro uses two panels. The left panel is similar to the left panel of Windows Explorer. It provides a listing of the categories: connections, ports, components, etc. The right panel is the information panel, which gives the specific data about any category highlighted in the left panel.

The panels look like the following:



My Security

- Firewall
 - Network Activity
 - Used Ports
- Proactive Protection
 - Process Activity
 - File and Registry Activity
- Web Control
 - Online Activity
- Event Viewer

[Switch to Simple View](#)

Firewall

Firewall is a key part of your system's protection. It monitors all the network traffic the system sends and receives, and it detects and prevents any attempted hacker attacks from outside the network leaving intruders no possibility of compromising your computer.

Firewall	Enabled: Rules Wizard
Network attacks blocked	0
Applications online	4
Total bytes sent	15.35 KB
Total bytes received	289.07 KB

Attacks Blocked

Date/Time	Attack Type	Attacker Address	Action
-----------	-------------	------------------	--------

For your convenience, Outpost Firewall Pro allows switching between simple and expert views of the main window depending on your needs and abilities to manage security products. If you select the **Simple** mode while installing the product and creating its configuration, the product will display its **Simple View**; if you specify the **Expert** level, the **Expert View** will be displayed. If you are not an advanced user, it would be easier for you to use the **Simple View** of the screen, as it does not contain any pages that might be difficult to understand. If you are an advanced user, we recommend switching to **Expert View**, which will provide you with more information about the product's operation and system performance. That could be useful for tracking system activity and taking steps if anything happens.

To switch between views, click **Switch to Expert View** or **Switch to Simple View** at the bottom of the left panel.

Note:

- Switching between views does not influence the functionality provided by the product.

As with Windows Explorer, any line that starts with a plus sign (+) can be expanded to show its subcategories. Any line starting with a minus sign (-) indicates the line has already been expanded and by clicking the minus sign, all of that line's subcategories will be hidden (to conserve screen space).

The left panel lists and the information panel display the details of the following categories:

- Firewall**

Selecting this category in the left panel displays general information about the firewall, such as its present state, policy, attacks detected and general statistics on open connections. When expanded, this category lists the following nodes:

- *Network Activity*

Lists all applications and processes that have active connections and the details of those connections.

- *Used Ports*

Lists all applications and processes having currently used ports for a network connection.

- **Proactive Protection**

Displays general information about Proactive Protection components, such as the Anti-Leak protection level, System Guard, Application Guard, and File & Folder Lock statuses, self-protection status and some general statistics.

- *Process Activity*

Lists all local events currently in the system monitored by Proactive Protection.

- *File and Registry Monitor*

Allows to track all operations that a specific process performs over files and registry entries in real time.

- **Anti-Spyware**

Displays general information about the Anti-Spyware component operation modes and its malware signatures database status, as well as some general statistics on detected objects.

- *Quarantine*

Lists all objects placed in quarantine.

- **Web Control**

Displays general information about the Web Control component, such as its current status, its security level and general statistics on filtered content.


- *Online Activity*

Lists all content elements being processed by the filter.

- **Event Viewer**

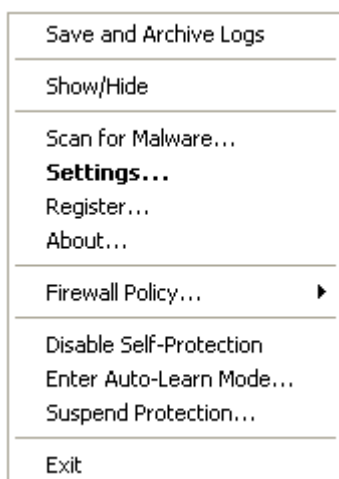
Displays detailed statistics for all past system and product activities by category.

2.3 System Tray Icon

By default, Outpost Firewall Pro automatically loads when Windows starts up to provide immediate protection of your system at the earliest stage. Once it is loaded, the icon with the white question mark on the blue shield  (Outpost Firewall Pro's default icon), is displayed in the system tray – the right end of the Windows task bar. When you see this icon, it means that Outpost Firewall Pro is operating and protecting you.

This icon is always available as a primary way you can access the product's controls, settings and logs. When you right-click on the system tray icon you get its context menu.

The system tray icon menu looks like the following:



The following commands are available on this menu:

- **Save and Archive Logs**

This command is only available if the **Log debugging information** parameter on the **Logs** tab of Outpost Firewall Pro settings is enabled. Updates Outpost Firewall Pro log files in the **Log** subfolder of the Outpost Firewall Pro's installation folder (*C:\Program Files\Agnitum\Outpost Firewall Pro* by default) and creates the *feedback.zip* archive containing all the log files.

- **Show/Hide**

Displays or hides Outpost Firewall Pro's main window.

- **Scan for Malware**

Starts a system scan for malware.

- **Settings**

Displays the **Settings** dialog window.

- **Register**

(Available only in a trial mode.) Allows to specify your registration key to get free annual Outpost Firewall Pro updates and support.

- **About**

Shows the current version of Outpost Firewall Pro and its database, lists each module in the package and their version numbers, and also provides license information.

- **Firewall Policy (or Enable Firewall)**

Opens a submenu where you can change Outpost Firewall Pro's firewall policy to one of these available modes: **Block All**, **Block Most**, **Rules Wizard**, **Allow Most**, and **Disable**. If the firewall is disabled, allows to enable it.

- **Disable Self-Protection (or Enable Self-Protection)**

Disables (enables) Outpost Firewall Pro self-protection.

- **Enter Auto-Learn Mode (or Leave Auto-Learn Mode)**

While in Auto-Learn mode Outpost Firewall Pro allows all applications' activities during a specified time period in order to create corresponding rules.

- **Suspend Protection (or Restore Protection)**

Disables (enables) Outpost Firewall Pro protection.

- **Suspend File & Folder Lock (or Resume File & Folder Lock)**

Disables (enables) Outpost Firewall Pro File & Folder Lock component.

- **Exit**

Opens a dialog that allows you to either close the GUI and stop the suite so Outpost Firewall Pro no longer protects your system or switch to background mode.

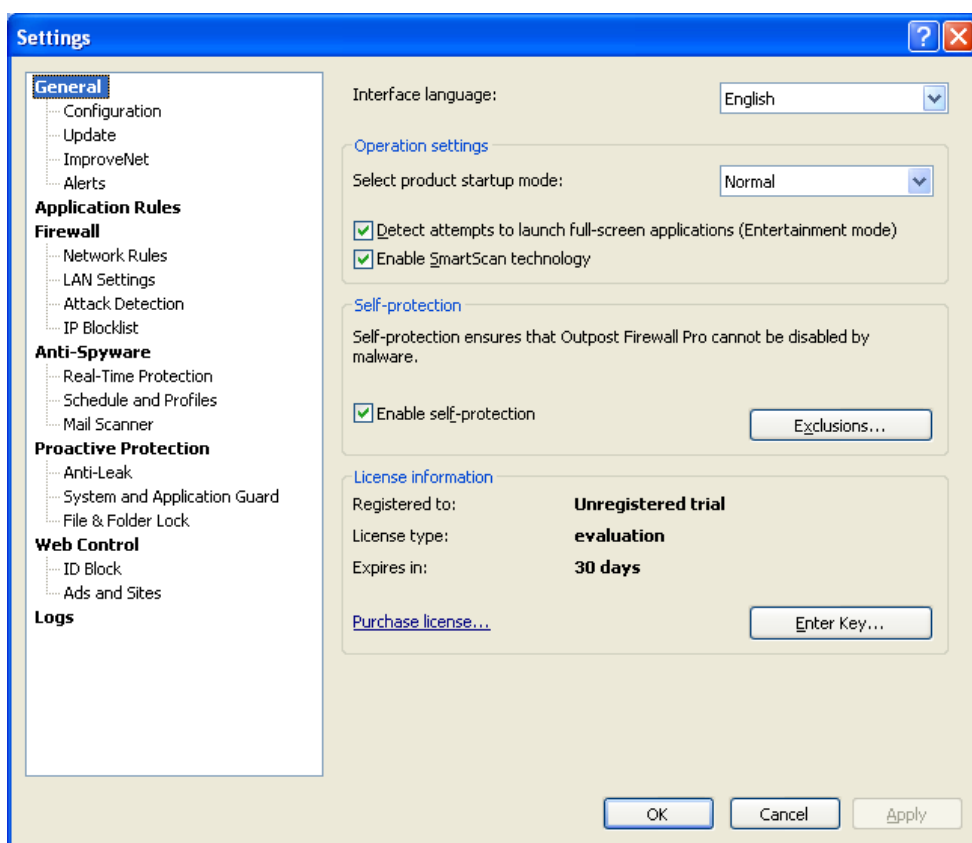
Note:

- The system tray icon is not visible while Outpost Firewall Pro runs in background mode.

2.4 Interface Language

The interface language is selected during the Outpost Firewall Pro's installation, but you can change it whenever you need to during Outpost Firewall Pro's operation. To do this:

1. Open the program's main window by double-clicking the system tray icon.
2. Click **Settings** on the toolbar.
3. Select the required language from the **Interface language** list.
4. Click **OK** to save the changes:




To activate the language change, you will need to restart Outpost Firewall Pro. The alert window that reminds you of this will be displayed after you click **OK** after step 4.

3 Basic Configuration

Outpost Firewall Pro is operating as soon as it is installed. Its default settings are optimized for most purposes and are recommended until you become fully acquainted with Outpost Firewall Pro, at which point you can customize it to best suit your particular needs.

This section gives a brief overview of Outpost Firewall Pro's basic controls a novice user should know about when starting to use the product, such as: how to start and stop the protection, how to create a new configuration, how to protect your settings from unauthorized alteration and how to specially designed Entertainment mode lets you stay protected while gaming online.

3.1 Starting and Stopping Protection

By default, Outpost Firewall Pro is automatically loaded when your computer starts up providing immediate protection at the earliest stage possible. Once it is loaded, the default icon with the white question mark on the blue shield  is displayed in the system tray, the right end of the Windows task bar. When you see this icon, it means that Outpost Firewall Pro is operating and protecting you.

Double-click the icon to open Outpost Firewall Pro's main window. To close the main window, click the X in the right-upper corner of the window, which does not shut down the product, but simply minimizes it, the product icon remains in the system tray indicating that it is running and protecting your system.

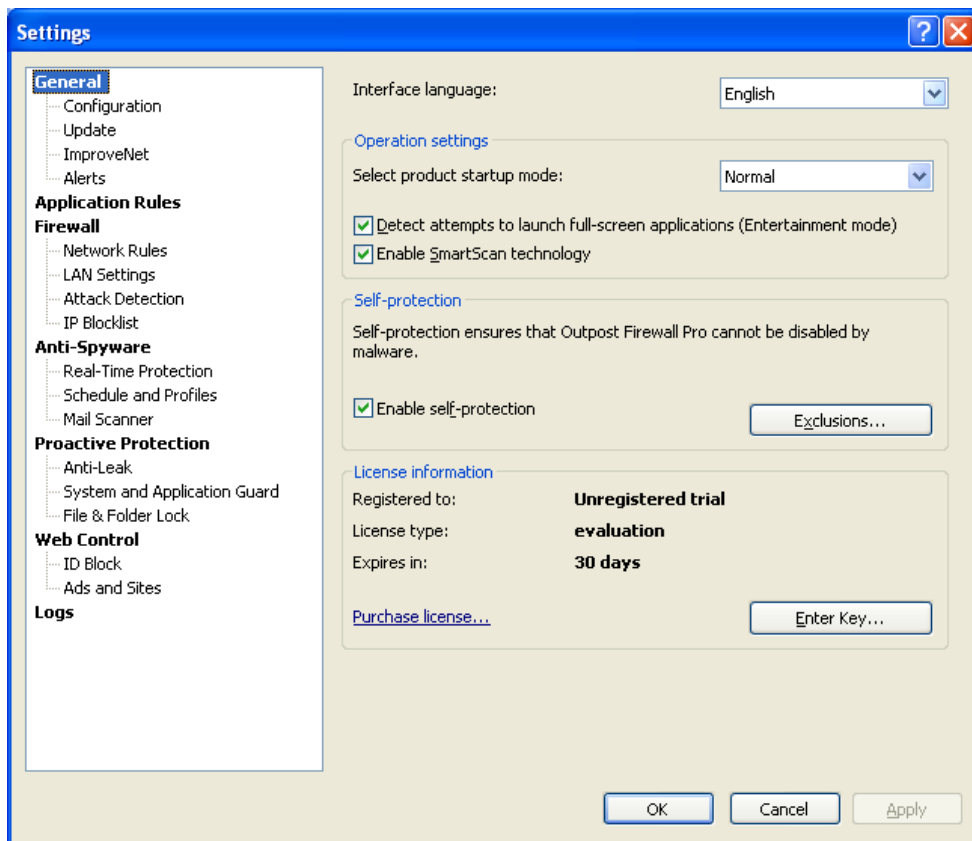
To completely stop Outpost Firewall Pro so it no longer protects your system, right-click the Suite's icon in the system tray, click **Exit**, select **Exit Outpost Firewall Pro and shutdown service** from the list.

Startup mode

Outpost Firewall Pro allows you to control its behavior when your system starts 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 parameters** section:

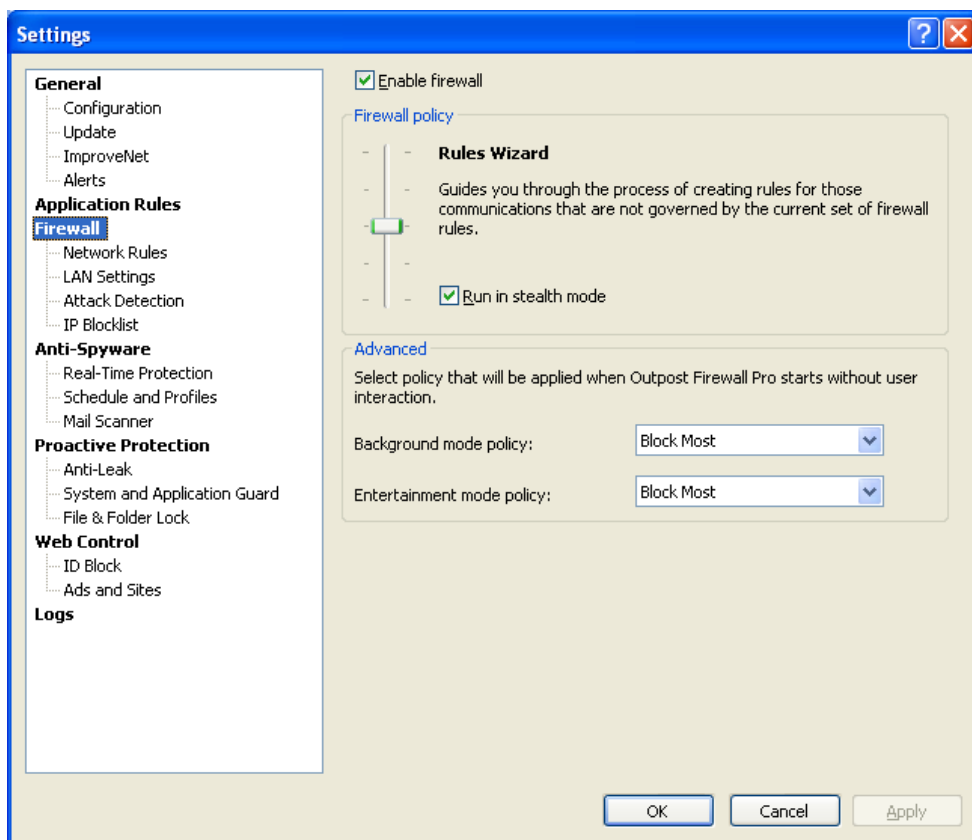
- **Normal** - the default mode. Loads Outpost Firewall Pro automatically when you turn on your computer and displays its icon in the system tray.
- **Background** - when in background startup mode, Outpost Firewall Pro runs invisibly without displaying its system tray icon or any of its dialog windows. This makes the suite invisible to users, which lets parents and system administrators block unwanted traffic or content in a way that's completely hidden from the user.

Another reason to use background mode is if you need to save system resources:



Note:

- Because Rules Wizard policy is not supported when Outpost Firewall Pro runs in background mode (as background mode does not include interaction with the user), you need to specify what firewall policy is to be applied when Outpost Firewall Pro starts in background mode. To specify the policy that should be applied in background mode, click **Settings** on the toolbar, select **Firewall**, and select the desired policy from the **Background mode policy** list:



You can manually start Outpost Firewall Pro at any time by selecting **Start > All Programs > Agnitum > Outpost Firewall Pro** and clicking **Outpost Firewall Pro**. To close Outpost Firewall Pro's GUI and switch to background mode, right-click the suite's icon in the system tray and click **Exit**.

- **Disable** - if this is selected, Outpost Firewall Pro will not run automatically at startup. Your system will not be protected until you manually start Outpost Firewall Pro.

3.2 Managing Protection Status

For security reasons, often it is crucial to know your protection status and to quickly define the mode each security module is in. The **My Security** page (the first page displayed when you double-click Outpost Firewall Pro's system tray icon) provides you with a list of critical product components and their current modes, so you can quickly evaluate a situation with single-click access to each component's settings in order to adjust Outpost Firewall Pro's behavior.

 All components are configured for optimal protection		
Component	Status	
Firewall	Enabled: Rules Wizard	
Real-time spyware protection	Enabled: Optimal	
Proactive protection	Enabled	
Web Control	Enabled: Optimal	
Spyware database	31.05.2010	
License	Trial, 30 days left	Purchase...

The following information about Outpost Firewall Pro's components is displayed:






- **Firewall.** Click the status link in the **Status** column to switch **Firewall** status. Clicking the policy name link will open the **Firewall** settings, allowing you to change its policy.
- **Real-time spyware protection.** Click the status link in the **Status** column to switch **Real-Time Protection** status. Clicking the protection level link will open the **Real-Time Protection** settings, allowing you to change them.
- **Proactive protection.** Click the status link in the **Status** column to switch **Proactive Protection** status.
- **Web Control.** Click status link in the **Status** column to switch **Web Control** status. Clicking the protection level link will open the **Web Control** settings, allowing you to change them.
- **Spyware database.** Clicking the **Update** link available in the case of an outdated database will start the update process.
- **License information.** Displays the type of license you have and if you are not registered yet, allows you to easily register the product by clicking the **Register** link.

If a component operates in a mode, which is different from the optimum (recommended), the corresponding line will be highlighted yellow to let you know that this component does not provide the required level of protection. If the component is disabled, the corresponding line will be highlighted red to let you know that this component currently does not protect you.

3.2 Selecting the Firewall Policy

One of the most useful and important features of the firewall is its network access policy. A policy is the basic behavior Outpost Firewall Pro uses to control your computer's access to and from the Internet or any other networks it may be connected to. The **Block Most** policy, for example, gives Outpost Firewall Pro a very suspicious attitude, but the **Allow Most** policy makes Outpost Firewall Pro very trusting.

Outpost Firewall Pro can function according to the following policies:

Icon	Policy	Description
	Block All	All network connections are blocked, both to and from your computer (except the local traffic).
	Block Most	All network connections are blocked except those that are explicitly allowed by global or application rules.
	Rules Wizard	Helps you determine how an application should interact with other software and computers the first time that application is run.
	Allow Most	All network connections are allowed except those that are explicitly blocked by global or application rules.
	Allow All	All network connections are allowed.

The icon (see the table above) of the active mode displays in the system tray as the Outpost Firewall Pro icon. That way you can tell at a glance what mode the firewall is in simply by looking at its system tray icon.

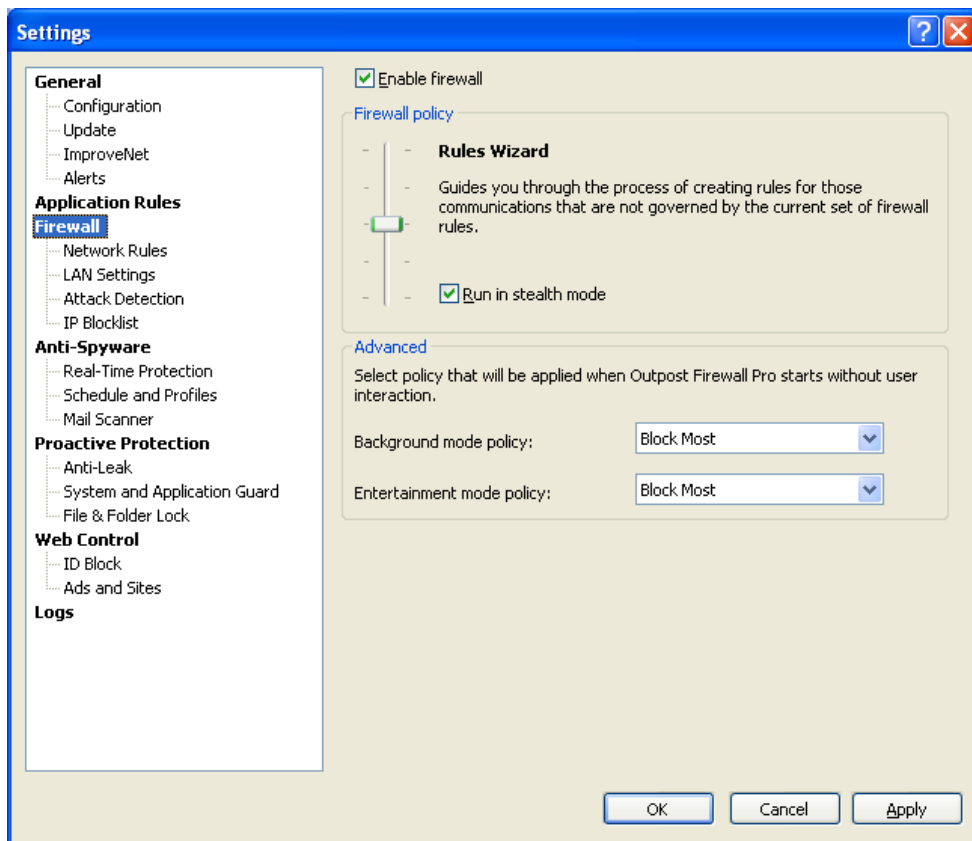
Note:

- If Outpost Firewall Pro operates in background mode, no icon is displayed.

Changing the firewall policy

To change the current firewall policy:

1. Click **Settings** on the toolbar.
2. Select the **Firewall** page.
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.

Important:

- If the firewall is disabled, Attack Detection is also disabled.

Running in stealth mode

By default, Outpost Firewall Pro is operating "stealthily", which means that your computer does not respond to port scans and silently blocks them, making itself invisible to hackers. Normally, when your computer receives a connection request to a port that is not used for any incoming or outgoing connections, it lets the other computer know that the port is not used by sending a "port unreachable" notification. In stealth mode, your computer will not respond, making it seem like it is not turned on or not connected to the Internet. In this case, packets sent to the unused port are simply ignored by the firewall without notifying the source via an ICMP or TCP message.

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

Note:

- It is recommended that you keep Outpost Firewall Pro in stealth mode unless you have some reason not to.

Note:

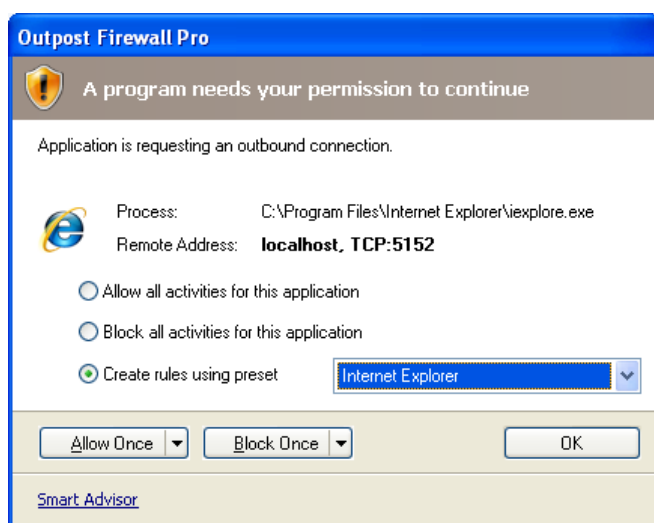
- Because the Rules Wizard policy is not supported when Outpost Firewall Pro runs in background or Entertainment mode (as these modes do not include interaction with the user), you need to explicitly specify what firewall policy is to be applied when Outpost Firewall Pro switches to one of these modes. See the corresponding links for details.

3.2.1 Running in Rules Wizard Mode

When Outpost Firewall Pro is first installed, the default policy is **Rules Wizard**. With this policy, Outpost Firewall Pro displays a prompt each time a new application or process (for which no rules are specified) requests network access or when an application requests a connection that is not covered by its existing rules. Thus Outpost Firewall Pro lets you decide whether an application should be allowed a network connection to a specific address and port.

Outpost Firewall Pro also lets you specify network parameters for each type of application. Instead of having to create a new (and often complex) rule each time a new application is run, Outpost Firewall Pro enables you to simply select a preset rule based on a similar well-known application. The firewall even recommends the best selection for you, so you simply have to okay Outpost Firewall Pro's recommendation, unless you are certain of a better choice.

The Rules Wizard prompt looks like the following:



The choices you can make for an application in **Rules Wizard** mode are as follows:

- **Allow all activities for this application**

This is only for applications you trust completely. All network requests by this application will be allowed.

- **Block all activities for this application**

This is for applications that should not be allowed network access. All network activities for this application will be disabled.

- **Create rules using preset**

This is for applications that can obtain network access using specific protocols, via particular ports, etc. This mode creates a rule or set of rules for the application that limits network access to those specific ports and protocols using predefined presets that are optimum for most purposes.

Select the required application from the drop-down list and click **OK** to make the firewall control the application according to the specific rules. You can also create your own rule for this application by selecting **Custom** from the list and specifying the rule settings.

Note:

- In the case that an application requests a connection to the server that has several IP addresses, Outpost Firewall Pro automatically detects all server addresses and configures the corresponding rules for all the server IP addresses according to the action you specify.

- **Allow**

Allows to select one of the following actions (click the down arrow on the **Allow** button to open the menu):

- **Allow Once**

The default action. This is for applications that you are doubtful of but would like to see what they do with network access. The connection will be allowed this one time. No rule is created for the application and the next time this application tries to establish a network connection, this same dialog window will appear.

- **Auto-Learn Mode**

Allows the connection and switches Outpost Firewall Pro to Auto-Learn Mode, where it creates allowing rules for all the requested connections.

- **Block**

Allows to select one of the following actions (click the down arrow on the **Block** button to open the menu):

- **Block Once**

The default action. This is for applications that you do not trust but do not want to block totally. The connection will be blocked this one time. No rule is created and the next attempt by this application to establish a network connection results in this same dialog window.

- **Block and Terminate**

Blocks the requested connection and ends the process that requested it. No rule is created and the next attempt by this application to establish a network connection during its next run results in this same dialog window.

- **Block and Add to Blocklist**

Blocks the requested connection and puts the remote IP address on the list of blocked IPs.

Note:

- Rules Wizard is not supported when Outpost Firewall Pro is run in background mode, as background mode does not include interaction with the user.
- For details on creating application rules, see [Managing Applications Network Access](#).
- If you need assistance with a decision when responding to a product prompt, click the **Smart Advisor** link to get advice on the current event.

3.2.2 Smart Advisor

During its operation, Outpost Firewall Pro constantly interacts with the user by means of 'learning dialog boxes', or prompts. These could appear, for example, when the program may behave differently than its

rules cover with an element or component or the requested connection has no rule and user response is needed.

To assist the user in making a decision, Outpost Firewall Pro provides additional information on the subject and suggestions which are available via the **Smart Advisor** link included in the prompt dialog. After clicking on **Smart Advisor**, a new window provides details for selecting Outpost Firewall Pro's activity, such as properties of an executable that requires a connection and a description of programs for which such activity could be typical along with advice.

3.3 Running in Auto-Learn Mode

To reduce the number of Rules Wizard prompts during the initial stage of Outpost Firewall Pro operation, you can set it to memorize (auto-learn) typical activities performed by a system by enabling the Auto-Learn mode.

In this mode, Outpost Firewall Pro assumes all new program activity is legitimate and consequently allows network access and process interaction to all requesting programs. As different programs access the Internet and interact with other software for the first time, Outpost Firewall Pro memorizes their identities and creates allowing rules for all the requested connections. The created rules will remain in effect after the auto-learn period expires and the computer is switched back to normal monitoring mode. If the rule exists for the requested connection, the connection is managed according to these created rules, so your programs will continue to be able to access the Internet without triggering a "new connection" prompt.

To enable the Auto-Learn mode, right-click the Outpost Firewall Pro system tray icon and select **Enter Auto-Learn Mode**. Specify the period of time you want Outpost Firewall Pro to be trained and click **OK**.

After the specified period, the software automatically enables rules autocreation and updates so the network traffic is processed according to rules created during the auto-learn period and any rules based on the factory presets.

To switch back to normal mode before the specified period is over, right-click the Outpost Firewall Pro system tray icon and select **Leave Auto-Learn Mode**.

Note:

- Auto-Learn Mode can pose a security risk because allowing rules are created for every requested connections. So while in Auto-Learn mode, be sure you are not running any unknown or untrusted applications and not visiting objectionable sites.

3.4 Running in Entertainment Mode

When playing games or watching movies you probably want to avoid product prompts and alerts from distracting your attention or capturing focus, yet still want to be protected, especially when playing online.

Outpost Firewall Pro provides a specially designed **Entertainment mode** where protection is active without bothering users with numerous product prompts and alerts. Once the full screen application (a game, media player, etc.) is started, Outpost Firewall Pro detects this event and suggests entering Entertainment mode, so the application runs using the Entertainment mode policy (see below), in which case no alerts and messages are displayed with the full screen application, updates are not checked for, and scheduled scans are not performed.

To set Outpost Firewall Pro to detect full-screen applications and to have it suggest switching to Entertainment mode, click **Settings** on the toolbar and select the **Detect attempts to launch full-screen applications (Entertainment mode)** check box. To set the Entertainment mode policy, click the **Firewall** tab and select the policy from the corresponding list. This firewall policy will be applied each time Outpost Firewall Pro enters Entertainment mode and will be switched back to what it was before when Entertainment mode no longer needed.

The Entertainment mode prompt looks like the following:



To enable or disable Entertainment mode for specific applications by clicking **Settings** on the toolbar, selecting the **Application Rules** tab and double-clicking the required application. On the **Options** tab, select the necessary action from the **When application is entering full-screen mode** list:

Note:

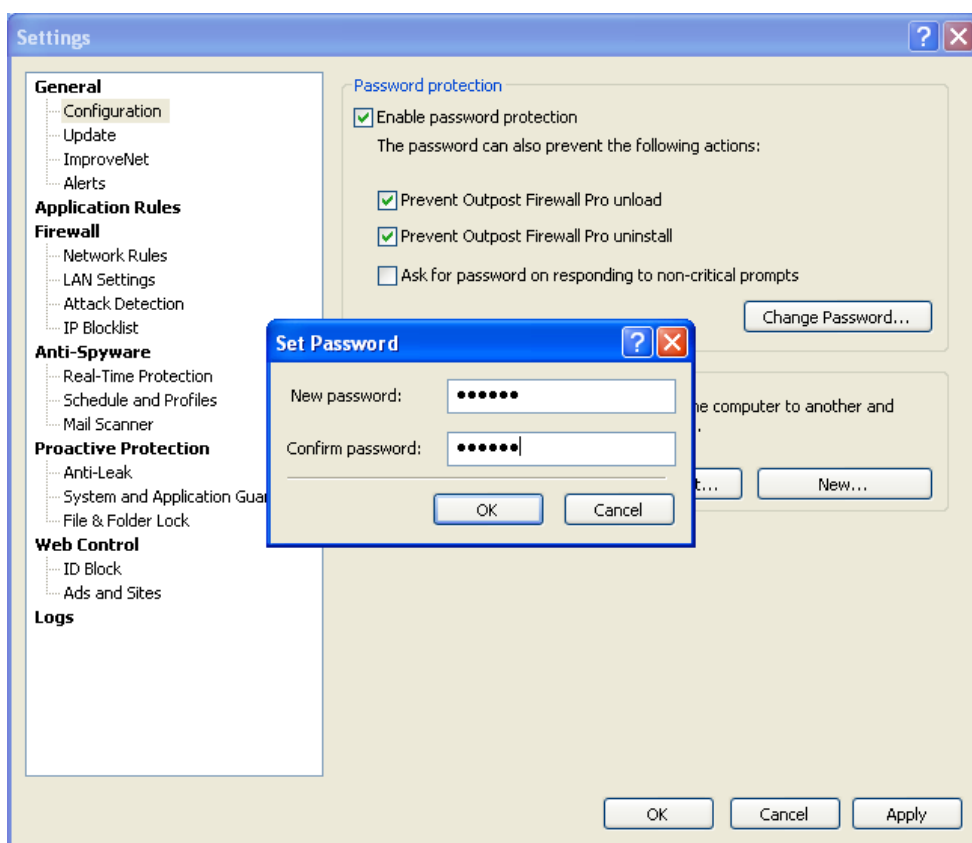
- When operating in background mode, Outpost Firewall Pro does not need to enter Entertainment mode.

3.5 Protecting Configuration with a Password

Outpost 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. You can, for example, block access to objectionable sites for your children and know that 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:



Specify the password in its dialog box, confirm it and click **OK** to save it. Click **OK** and Outpost Firewall Pro will start to protect its settings. After that, every time somebody tries to gain access to the product settings or to create a new configuration, he will be prompted for this 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** twice.

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.

You can additionally protect Outpost Firewall Pro from being unloaded and uninstalled by selecting the corresponding check boxes. This prevents unauthorized persons from disabling your protection and the restrictions you set and is most useful for parents who want to control their children's Internet access and employers who need to restrict the activities of their employees.

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

Note:

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

4 Updating Outpost Firewall Pro

Security updating is one of the key maintenance procedures you should undertake regularly on your computer. Because new malware appears often, the benefits of having an updated, well-configured security solution far outweigh the time it takes to run an update. Updating not only enlarges the spyware database, but also addresses previous software version issues found by users and specialists and corrected or enhanced by the product developers. New opportunities for product performance appear. Considering that you can do most updates automatically in the background, there's really no reason to not have properly updated software.

Outpost Firewall Pro's update is 100% automatic, including downloading the updated components, installing those files and modifying the registry. Because it is vitally important for your security to use the latest technologies, updating Outpost Firewall Pro was made to be as simple and automatic as possible.

By default, updates are checked every hour. If you need to download updates immediately, click **Update** on the toolbar. Outpost Firewall Pro Update wizard will perform all the necessary tasks, downloading the latest available product components, presets and malware signatures database. After the process is complete, click **Finish**. You can also manually perform updates at any time by clicking **Start > All Programs > Agnitum > Outpost Firewall Pro > Update**.

Agnitum lets you change the regular updates schedule and suggests that you personally may want to help in updating Outpost Firewall Pro's rules by participating in a completely free Agnitum ImproveNet program.

Note:

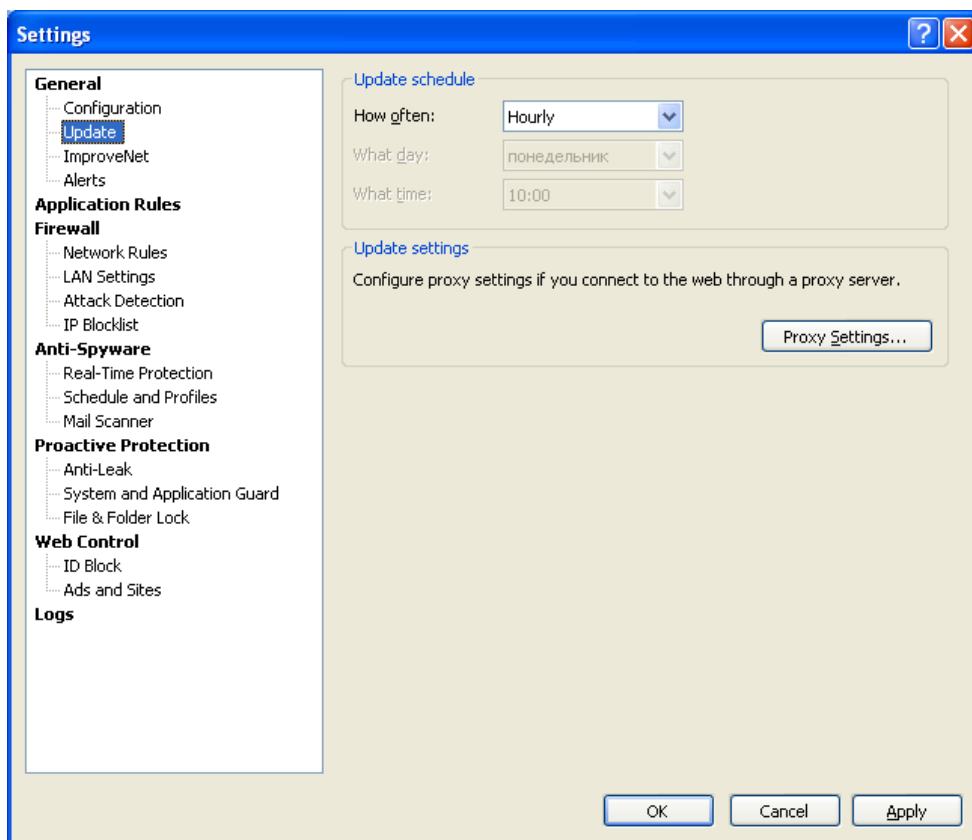
- The current Outpost Firewall Pro version and modules list are available at the **Update** page of the product settings.

4.1 Configuring Updates

To configure Outpost Firewall Pro updates, click **Settings** on the toolbar and select the **Update** page.

Schedule

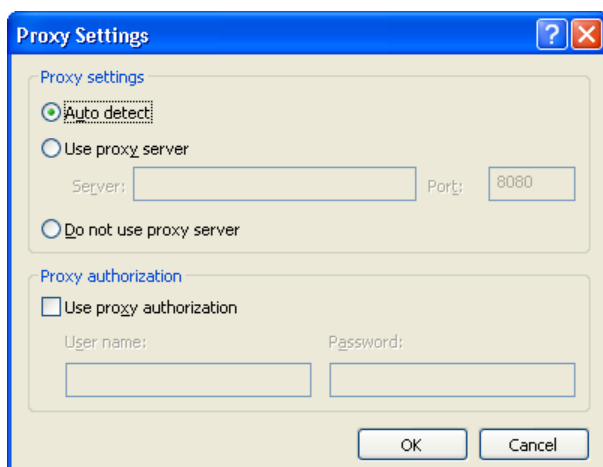
By default, updates take place on an hourly basis, however, you can choose a time when Outpost Firewall Pro downloads updates on your own. To do this, click the **Settings** button on the toolbar and select the **Update** page:



Under **Update schedule** you can specify how often updates are to be downloaded by selecting the desired frequency in the **How often** list. If you select weekly updates, you can also specify a day for updating and the exact time when the product will download updates. If you select daily updates, you can specify the time of day to download updates. If you select **Manually**, updates will not be checked unless you click the **Update** button on the toolbar.

Proxy settings

If you connect to the Internet through a proxy server, you can set the connection settings by clicking **Proxy Settings** on the **Update** page of the product settings. You can specify the server and port number manually. To do so, select the **Use proxy server** option under **Proxy settings** and type in the server name and port number in the text boxes provided:



Along with specifying the proxy server, you can define whether it requires authorization by selecting the **Use proxy authorization** check box under **Proxy authorization** and specify the access credentials (user name and password).

If (when connecting to the Internet) your computer uses a proxy server, but you want the updating process to be performed directly from the product developer's server, select **Do not use proxy server**.

If you do not use a proxy server, you can select either **Do not use proxy server** or the **Auto detect** option.

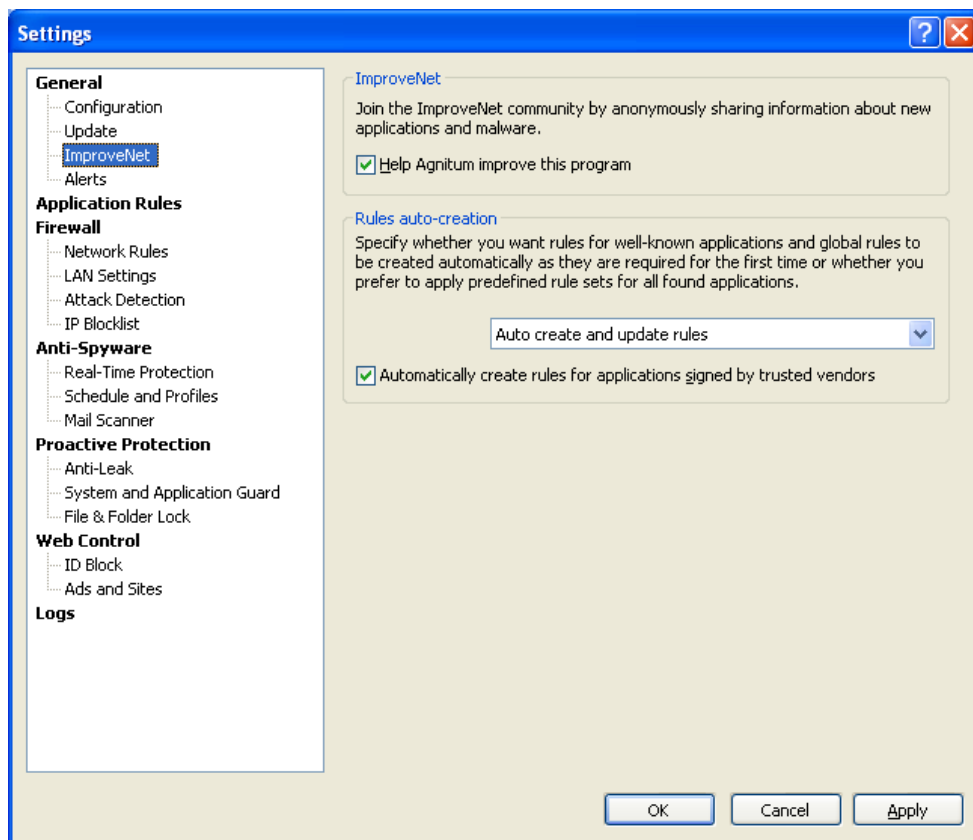
4.2 Agnitum ImproveNet

We invite you to contribute to a safer Internet through the free and cooperative Agnitum ImproveNet program to improve the quality, security and control features of Agnitum products. There is no work on your part. You simply agree to have some non-personal data anonymously collected each week to expand Outpost Firewall Pro's database of known applications, so that many more automatic rules are available to you. This will reduce the number of dialog pop-ups that require your attention.

With your consent, Outpost Firewall Pro will collect information only about applications on your computer. The data are collected completely anonymously, what means that neither name, address, network identification, nor any other personal or identifying information will be collected of any kind whatsoever. Outpost Firewall Pro simply collects data on network-enabled applications for which no rules presently exist, any new system rules created, and general application usage stats. The information is compressed and sent once a week to Agnitum as a background process so your computer use is not interrupted or disturbed in any way.

After a new rule has been received and validated by Agnitum, it is automatically shared with all other Outpost Firewall Pro users via update along with other product updates.

To help us better serve the Internet community, please join the Agnitum ImproveNet program. Simply click **Settings > ImproveNet** and select the **Help Agnitum improve this program** check box. You can disable this feature at any time simply by clearing this check box:



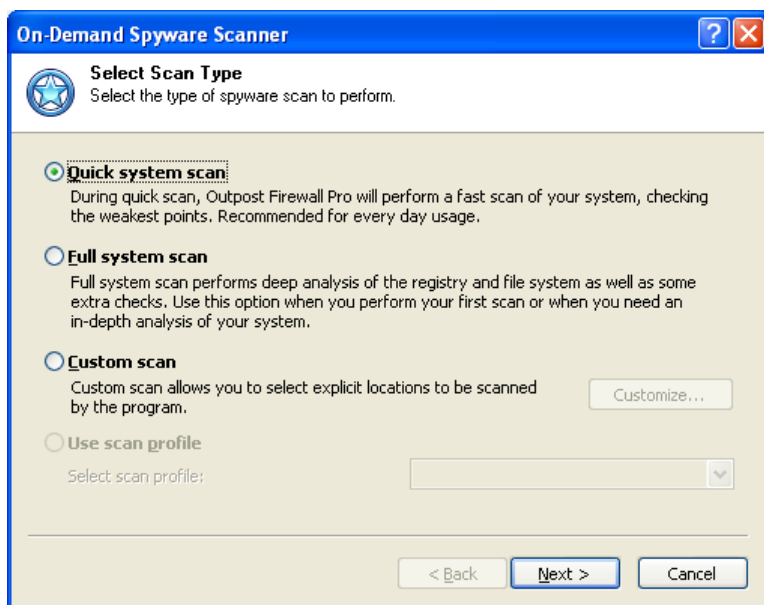
5 Performing a System Scan

On-demand global system scanning lets you scan for and remove threats on hard disks, network folders, DVDs, and external storage devices at your own convenience. By excluding locations and file types from the scan (provided you are certain these locations and/or file types are not vulnerable to infection), you can flexibly specify scan areas to meet your specific requirements.

It is recommended to run a full scan just after Outpost Firewall Pro's installation to check your system for whatever malware it already has on it. To do this, start **On-Demand Malware Scanner** by clicking the **Scan** button on the toolbar. You can also start the scanner with the main window closed by right-clicking the system tray icon and selecting the **Scan for Malware** option. The wizard will help you specify the scan settings and guide you through the whole process of the system scan.

5.1 Selecting Scan Type

The first step lets you select the type of system scan. The following options are available:



- **Quick system scan.** This option performs a fast scan of your system by checking only the most vulnerable points such as running processes in memory, susceptible registry keys, and target files and folders. This option is recommended for every day usage.
- **Full system scan.** A full system scan is a deep analysis of the registry and file system as well as some extra checks (processes in memory check, cookies scan, startup entries scan). This check should be performed when you scan your system the first time. The operation can take considerable time depending on the speed of your processor, the number of applications you have on your computer and the amount of data you have on your drives.
- **Custom scan.** This option enables you to explicitly select the locations to be scanned. You can select either of the options above or you can choose specifically what to scan on your file system.
- **Use scan profile.** This option allows you to select a custom scan profile you created. This option is available only if at least one scan profile exists.

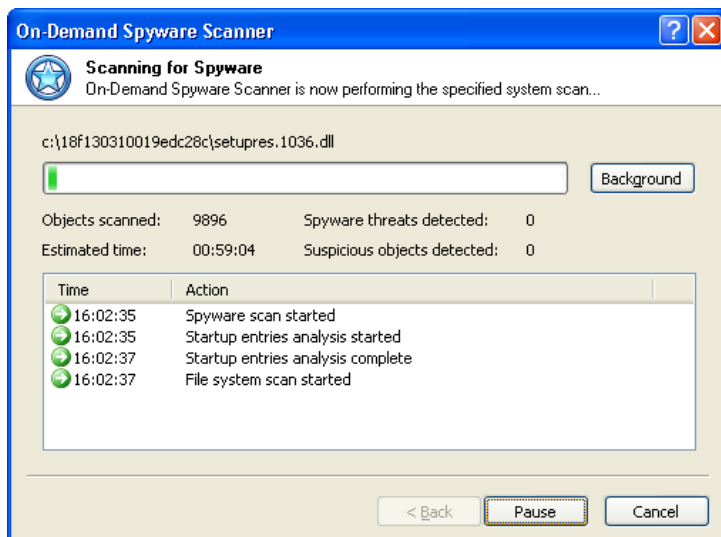
Tip:

- To improve scan performance, you can have Outpost Firewall Pro create scan status cache files in each scanned folder by selecting the **Enable SmartScan technology** check box on the **General** tab of the product properties. Note, that the cache files are invisible and therefore may cause false positives from anti-rootkit tools.

After selecting the scan type and, if necessary, the scan profile name, click **Next** to proceed.

5.2 Scanning Specified Locations

After clicking **Next**, Outpost Firewall Pro starts to scan the selected objects and locations. The progress step displays the following stats as the scan continues: the total number of objects scanned and the number of detected potentially malicious objects:



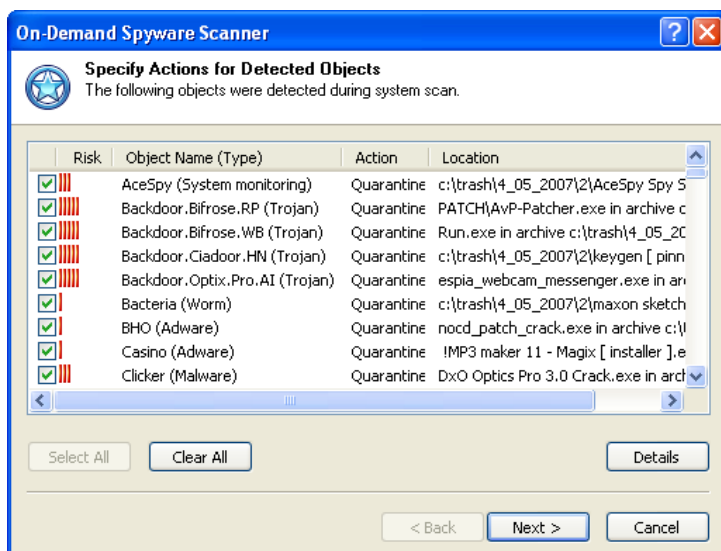
The scanning process can run in background mode. If you want to work with Outpost Firewall Pro while the scan is underway, click the **Background** button and the wizard will be minimized. To see the full window again, select **Anti-Spyware** on the left panel of the main window and click **Show Details** on the Information panel.

To abort a scan and see its results at any time, click **Cancel**.

When the scan is complete, a list of detected objects (if any are found) is displayed automatically. If your system is clean (i.e. no suspicious objects were found), only the stats of the scan are displayed.

5.3 Removing Detected Malware

The **Specify Actions for Detected Objects** step lets you view whatever malware was detected so you can remove it from your system. Next to each malware is displayed its degree of risk, the category it belongs to, and the action to be performed on it:



Double-click an object to see a listing of all the places on your computer where it is located.

To change the action, right-click the object and select the action from the shortcut menu.

Select the check boxes next to the objects you want to process and click **Next**. Outpost Firewall Pro then performs the specified actions – cures the object, removes it from the places it is registered in and from memory or places in quarantine so you can restore it later if you find some software won't work without it or you can delete it completely if all is well. While in quarantine, malware has no effect on your system. For details on using the spyware quarantine, see the User Guide.

Any software that you did not select will be left intact and will continue to be active on your system.

Tip:

- If you know that a found program is not malware but is in fact legitimate software and do not want to treat it as spyware or a virus (for example, in order to use a freeware application, it must display its ads from a particular adware program), you can add such programs to the exclusions list. Outpost Firewall Pro will ignore the programs on the exclusions list and will display no alerts when detecting their activity. Also, these programs will not be displayed on the list of detected spyware.

You can also specify files and folders, which Outpost Firewall Pro should not scan for malware.

To add a detected item to the exclusions list, right-click its name and select either **Add Spyware to Ignore List** or **Add File to Ignore List** correspondingly.

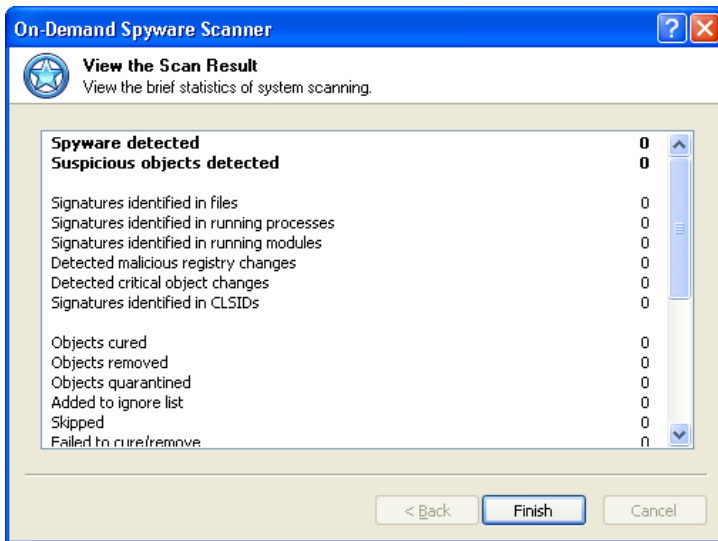
You can later remove items from the exclusions lists using the **Exclusions** button on the **Anti-Spyware** dialog page of the product **Settings** window.

Important:

- A cookie is not spyware, but it can be used as a holding file to transfer private information from your computer to a specific web site. Spyware programs installed on your computer can write your private information into cookie files, which can later be read by the site that owns those cookies the next time your browser visits that site (whether you knowingly go to the site or your browser is simply directed there).

5.4 Viewing Scan Results

The last step of the wizard displays a scan report where you can see the number of detected, cured, removed, and quarantined malware and other details. After viewing the results, click **Finish** to close the wizard:



Note:

- To see the objects that the Anti-Spyware component detected and removed, open the **Event Viewer** section in the left panel of Outpost Firewall Pro main window and select the **Anti-Spyware** log.

6 Uninstalling Outpost Firewall Pro

To uninstall Outpost Firewall Pro:

1. Right-click the Outpost 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 Agnitum **Outpost Firewall Pro** and click **Remove**.
4. Click **Yes** to confirm the removal.

The program will ask you to optionally send a feedback report, so you can specify the reasons for its removal. This will help the developers improve further product versions.

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

Note:

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

7 Troubleshooting

If you need assistance in working with Outpost Firewall Pro, please visit the Agnitum support page at <http://www.agnitum.com/support/index.php>. Among available support options are the knowledge base, documentation, support forum, product-related web resources, and direct contact with support engineers.

About Agnitum

Agnitum offers three headline products - Outpost Firewall Pro - a standalone firewall solution securing personal and family desktops, Outpost Security Suite Pro – an all-in-one product comprised of the award-winning firewall, antivirus, antispymware, antispam and integral host protection, for home users, and Outpost Network Security, ensuring a reliable endpoint protection and performance of the corporate network. Agnitum delivers computer security solutions to home PC users as well as small and medium businesses.

Operational Office:

194044,

Bolshoy Sampsonievskiy 60, Liter "A"

St.Petersburg, Russia

HQ address:

Acropoleos Avenue

8 Mabella Court

Nicosia, Cyprus