



OUTPOSTPRO

SECURITY SUITE

Getting Started

Abstract

This document provides a quick start reference to orientate a first time user in the basic concepts and operations of Outpost Security Suite Pro 2009. It also gives some of the primary ways a user might want to customize Outpost Security Suite Pro to fit his or her preferences.

Table of contents

1 Installing and registering Outpost Security Suite	4
1.1 System Requirements.....	4
1.2 Installing Outpost Security Suite Pro	4
1.3 Registering Outpost Security Suite Pro	10
2 User Interface and Controls Basics.....	12
2.1 The Toolbar	12
2.2 Left and Information Panels	13
2.3 System Tray Icon	15
2.4 Interface Language	16
3 Basic Configuration.....	17
3.1 Starting and Stopping Protection	17
3.2 Managing Protection Status.....	19
3.3 Selecting the Firewall Policy	19
3.3.1 Running in Rules Wizard Mode.....	21
3.3.2 Smart Advisor	23
3.4 Running in Auto-Learn Mode.....	23
3.5 Running in Entertainment Mode	23
3.6 Protecting Configuration with a Password	25
4 Updating Outpost Security Suite Pro	27
4.1 Configuring Updates.....	27
4.2 Agnitum ImproveNet	29
5 Performing a System Scan	30
5.1 Selecting Scan Type	30
5.2 Scanning Specified Locations.....	31
5.3 Removing Detected Malware	31
5.4 Viewing Scan Results.....	33
6 Filtering Junk E-Mail	34
6.1 Enabling Spam Filter.....	34
6.2 Training Anti-Spam Filter	34
6.3 Manual Training	35
6.4 Automatic Training	35
7 Uninstalling Outpost Security Suite Pro	37
8 Troubleshooting	38
About Agnitum	39

1 Installing and registering Outpost Security Suite

1.1 System Requirements

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

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

Anti-Spam supports the following mail clients:

- Microsoft Outlook 2000, 2002 (XP), 2003, and 2007;
- Microsoft Outlook Express 5.0, 5.5, and 6.0;
- Vista Mail;
- The Bat!

Note:

- Outpost Security Suite 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 Security Suite Pro should not be run with any other security software. Running Outpost Security Suite 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 Security Suite Pro

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

To start the installation program of the Outpost Security Suite Pro system:

1. **Very Important!** Before installing Outpost Security Suite 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 OutpostSecuritySuiteProInstall.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 (OutpostSecuritySuiteProInstall.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\OutpostSecuritySuiteProInstall.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.

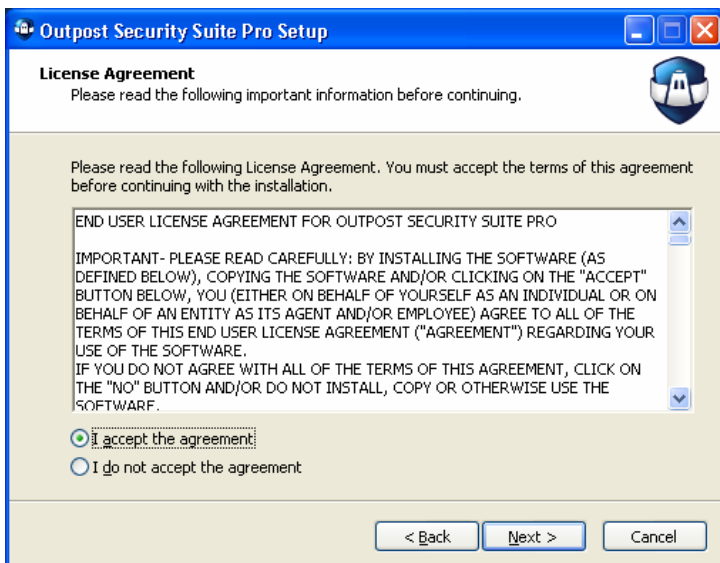


Choose the language for Outpost Security Suite Pro interface and click **OK**. Setup will display the **Welcome** dialog presenting basic features of the product:

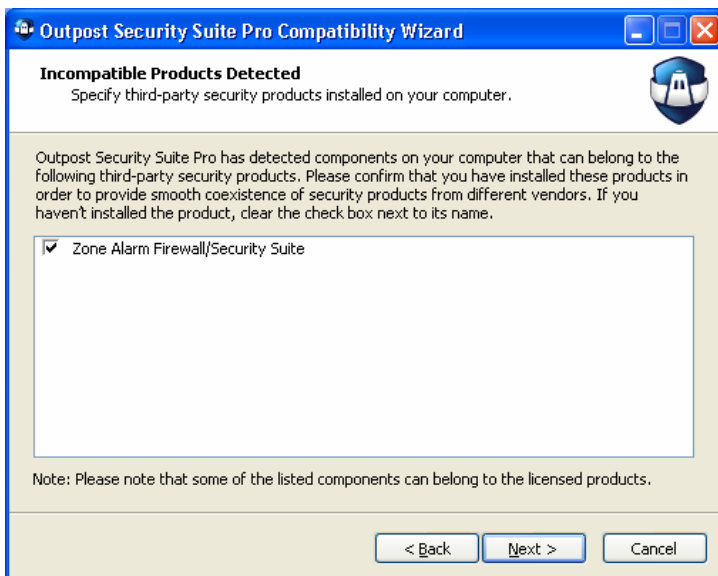


After clicking the **Next** button you will be asked to accept the License Agreement to use the **Outpost Security Suite Pro**.

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:



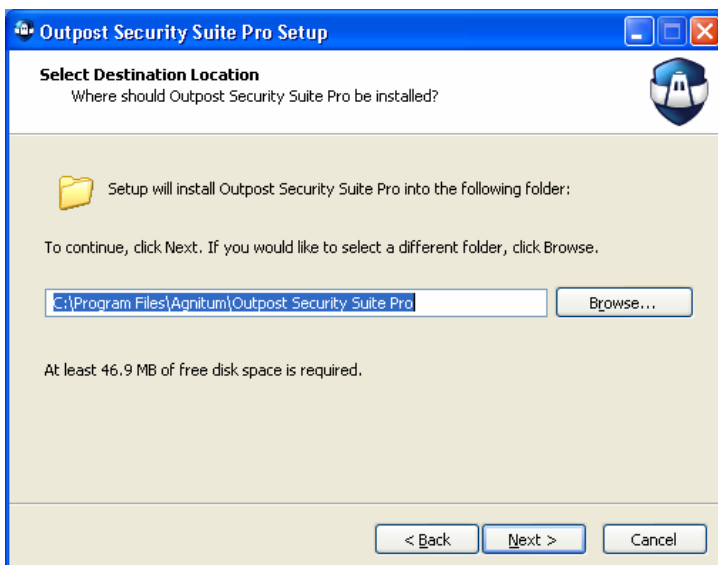
In case you have not removed any third-party security software, the setup wizard will display a prompt pointing at detecting incompatible software:



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

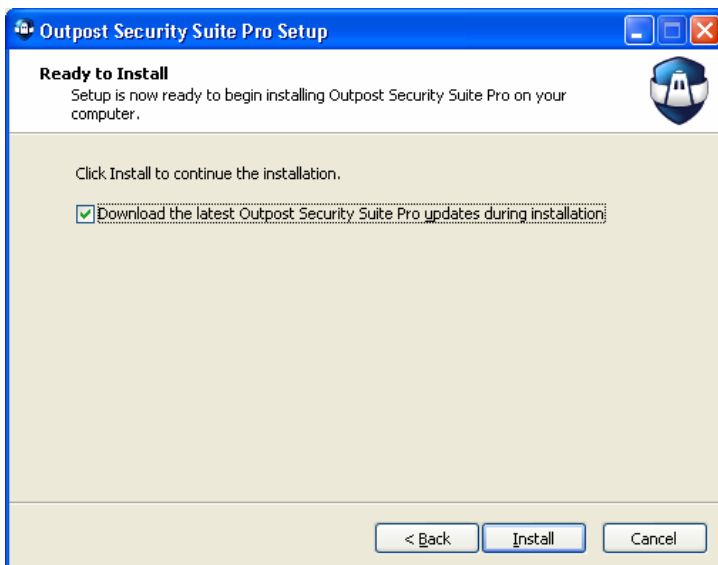
On detecting *a partly compatible product* the wizard will offer you one of the possible options to apply to the product.

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 Security Suite Pro files. You can use the default folder or select it manually.

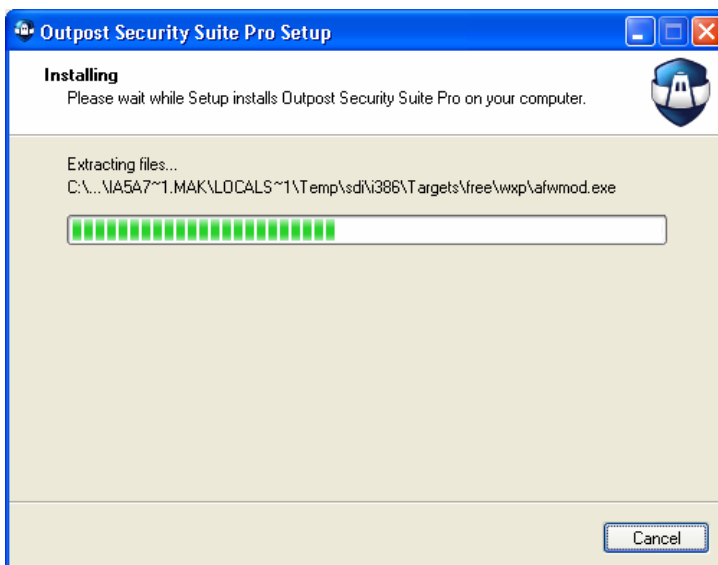
If you want to change the default file location, click **Browse**. Select the folder or create your own one and click **OK**. Click **Next** to proceed to the last step before actual installation:



Select the **Download the latest Outpost Security Suite 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:

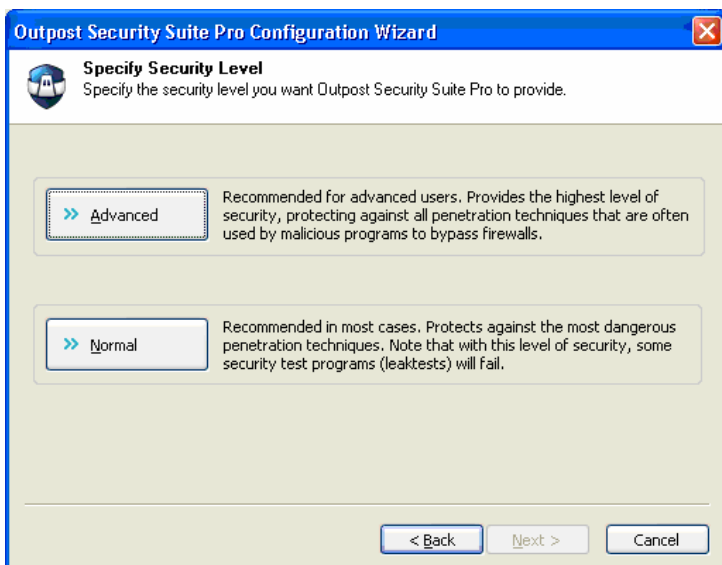


After the installation is finished, the **Configuration Wizard** will help you create a new configuration or import the previous if you install the product over an earlier version:



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 Security Suite Pro installation.

On creating a new configuration the setup wizard will offer you to select a necessary 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 of **Rules Autocreation** and **participating in the ImproveNet program**:

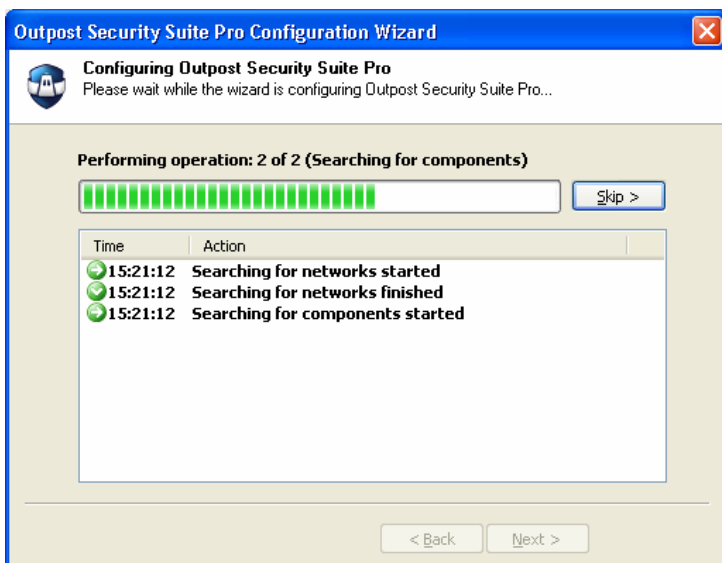


If you want to participate in the Agnitum ImproveNet program aimed at improving quality, security and control functions of Outpost Security Suite Pro, select the **Help Agnitum improve this program** option.

Rule autocreation allows you to enable rules autocreation, so that 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). You can select the necessary action from the drop-down menu.

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

After clicking **Next**, Outpost Security Suite 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 Security Suite Pro manually using the Start button menu or Windows Explorer right after installing it. You must reboot your computer before Outpost Security Suite Pro can start to protect your system.

1.3 Registering Outpost Security Suite Pro

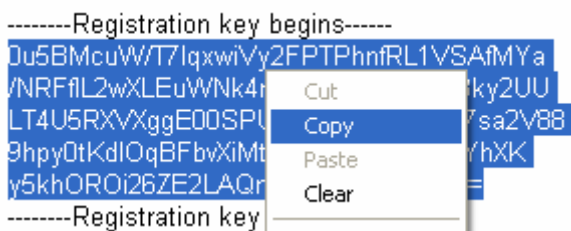
Outpost Security Suite Pro is available for your free evaluation. You are entitled to evaluate the software during the trial period with no obligation to pay. After the trial period, if you decide to keep the software and would like to receive free annual updates, you must register your copy with us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

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

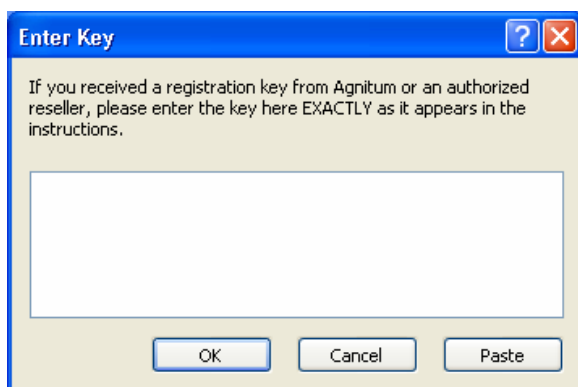
If you downloaded your copy from Agnitum's web site, to register your version, you need to purchase your registration key. Follow the instructions on the page <http://www.agnitum.com/purchase/outpost/> and you will receive your registration key by e-mail.

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 Security Suite 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 Security Suite Pro license, you actually get two licenses:

- A license for Outpost Security Suite Pro usage (lifelong);
- A license for free upgrades and support for one year (including the latest Outpost Security Suite 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 Security Suite Pro. To purchase a renewal, visit this page: <http://www.agnitum.com/purchase/renewal/index.php>.

Note:

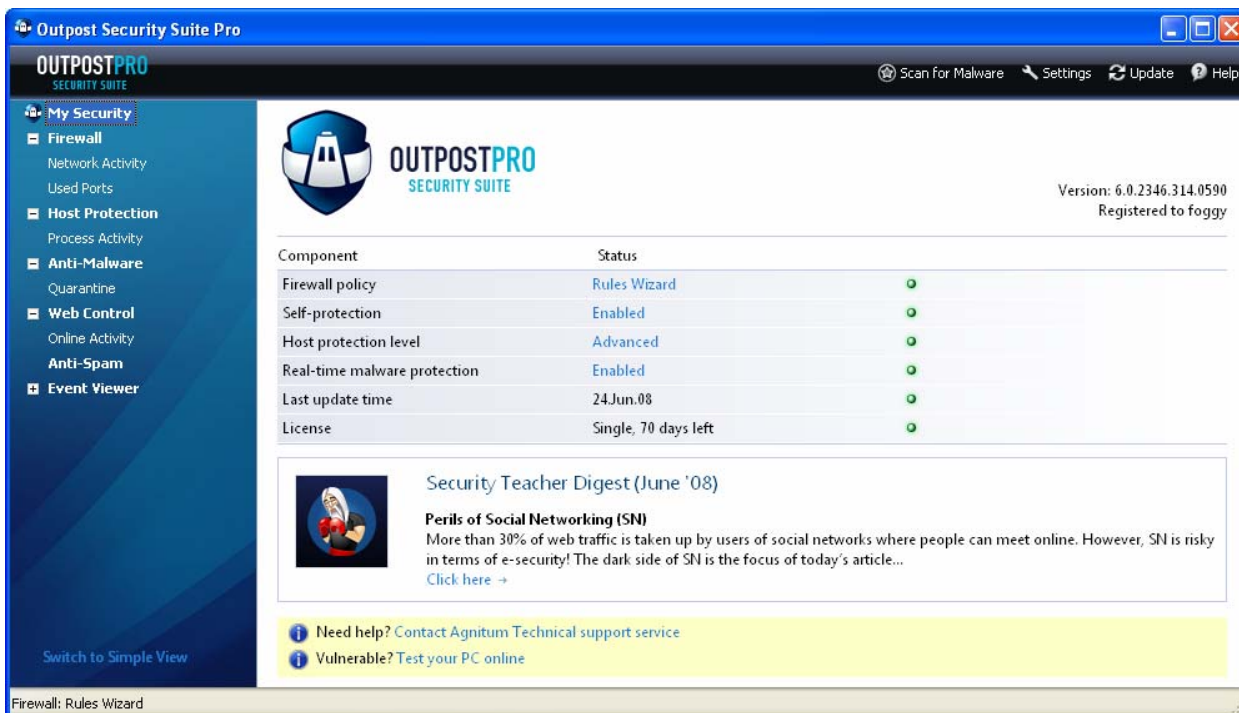
- Outpost Firewall Pro and Outpost Security Suite Pro are independent products and their registration keys are not interchangeable. It means that Outpost Firewall Pro registration key is not applicable to Outpost Security Suite Pro and visa versa. Please, be sure you are entering the correct registration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

2 User Interface and Controls Basics

When you launch Outpost Security Suite 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 Security Suite 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 Security Suite 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:

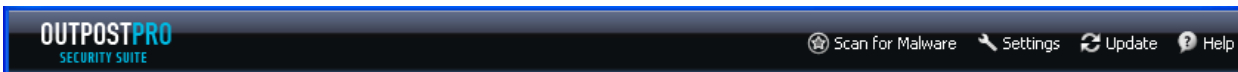
- **The toolbar**
- **Left panel**
- **Information panel**
- **Status bar**

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

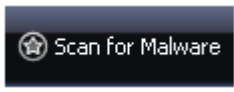
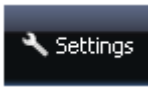
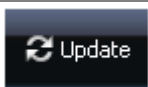
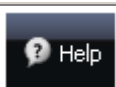
2.1 The Toolbar

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 Security Suite 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 Security Suite 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:



For your convenience, Outpost Security Suite 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 **Normal** security level while installing the product and creating its configuration, the product will display its **Simple View**; if you specify the **Advanced** 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.

- **Host Protection**

Displays general information about Host Protection, such as the local security level, Anti-Leak Control and Component Control statuses, self-protection status and some general statistics.

- *Process Activity*

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

- **Anti-Malware**

Displays general information about the Anti-Malware 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.


- **Anti-Spam**

Displays general statistics for all e-mail messages marked as spam or probable spam.

- **Event Viewer**

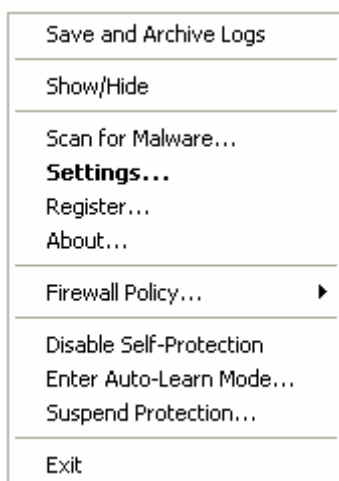
Displays detailed statistics for all past system and product activities by category.

2.3 System Tray Icon

By default, Outpost Security Suite 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 tower on the blue shield  (Outpost Security Suite 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 Security Suite 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 Security Suite Pro settings is enabled. Updates Outpost Security Suite Pro log files in the **Log** subfolder of the Outpost Security Suite Pro's installation folder (*C:\Program Files\Agnitum\Outpost Security Suite Pro* by default) and creates the *feedback.zip* archive containing all the log files.

- **Show/Hide**

Displays or hides Outpost Security Suite 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 Security Suite Pro updates and support.

- **About**

Shows the current version of Outpost Security Suite 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 Security Suite 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 Security Suite Pro self-protection.

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

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

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

Disables (enables) Outpost Security Suite Pro protection.

- **Exit**

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

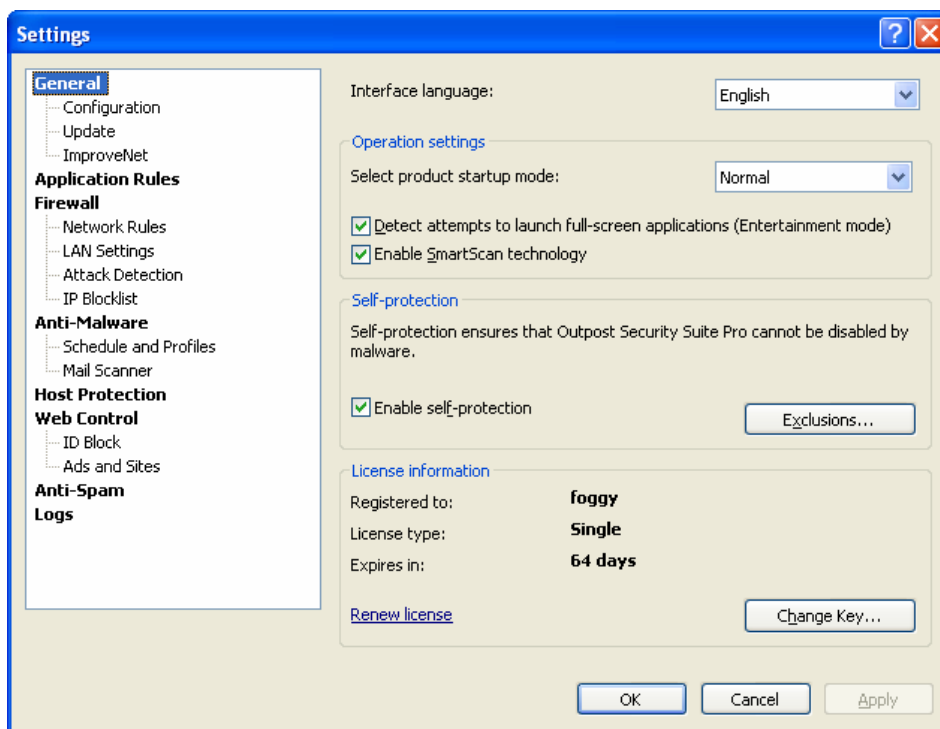
Note:

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

2.4 Interface Language

The interface language is selected during the Outpost Security Suite Pro's installation, but you can change it whenever you need to during Outpost Security Suite 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 Security Suite Pro. The alert window that reminds you of this will be displayed after you click **OK** after step 4.

3 Basic Configuration

Outpost Security Suite 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 Security Suite Pro, at which point you can customize it to best suit your particular needs.

This section gives a brief overview of Outpost Security Suite 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 Security Suite 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 tower 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 Security Suite Pro is operating and protecting you.

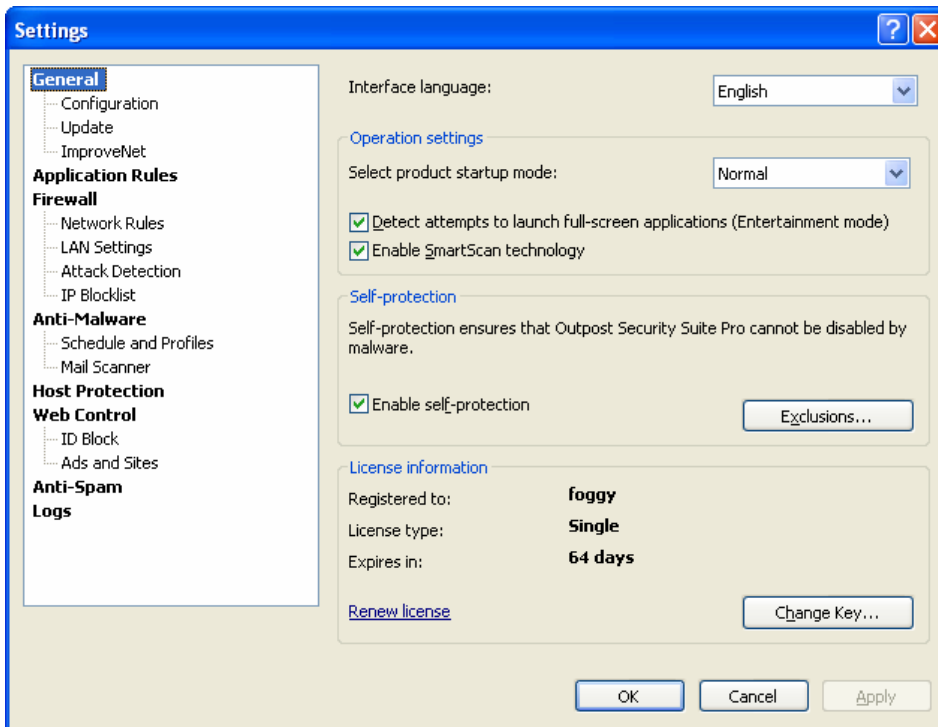
Double-click the icon to open Outpost Security Suite Pro's main window. To close the main window, click the X in the right-upper corner of the window, which does not shut down the product, but simply minimizes it, the suite icon remains in the system tray indicating that it is running and protecting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

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

Startup mode

Outpost Security Suite 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:

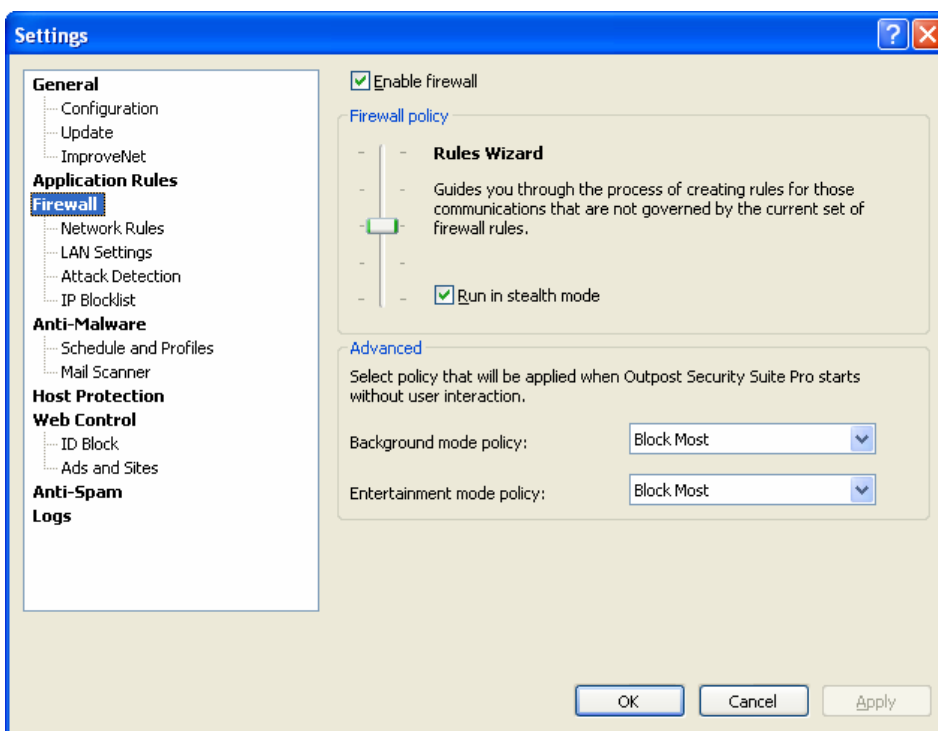
- **Normal** - the default mode. Loads Outpost Security Suite Pro automatically when you turn on your computer and displays its icon in the system tray.
- **Background** - when in background startup mode, Outpost Security Suite Pro runs invisibly without displaying its system tray icon or any of its 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 Security Suite 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 Security Suite 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 Security Suite Pro at any time by selecting **Start > All Programs > Agnitum > Outpost Security Suite Pro** and clicking **Outpost Security Suite Pro**. To close Outpost

Security Suite 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 Security Suite Pro will not run automatically at startup. Your system will not be protected until you manually start Outpost Security Suite 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 Security Suite 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 Security Suite Pro's behavior.

Component	Status	
Firewall policy	Rules Wizard	
Self-protection	Enabled	
Host protection level	Advanced	
Real-time malware protection	Enabled	
Malware database	10.Jun.08	
License	Single, 83 days left.	

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





- **Firewall policy.** Clicking the link in the **Status** column will open the **Firewall** settings, allowing you to change its policy.
- **Self-protection mode.** Clicking the link in the **Status** column will change the self-protection status.
- **Host protection level.** Clicking the link in the **Status** column will open the **Host Protection** settings, allowing you to change this level.
- **Real-time malware protection status.** Clicking the link in the **Status** column will open the Anti-Malware settings, allowing you to change them.
- **Malware database date.** 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.

3.3 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 Security Suite 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 Security Suite Pro a very suspicious attitude, but the **Allow Most** policy makes Outpost Security Suite Pro very trusting.

Outpost Security Suite Pro can function according to the following policies:

Icon	Policy	Description
	Block All	All network connections are blocked, both to and from your computer.
	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.

The icon (see the table above) of the active mode displays in the system tray as the Outpost Security Suite Pro icon. That way you can tell at a glance what mode the firewall is in simply by looking at its system tray icon. If Outpost Security Suite Pro is disabled, the icon turns red  and all network connections are allowed.

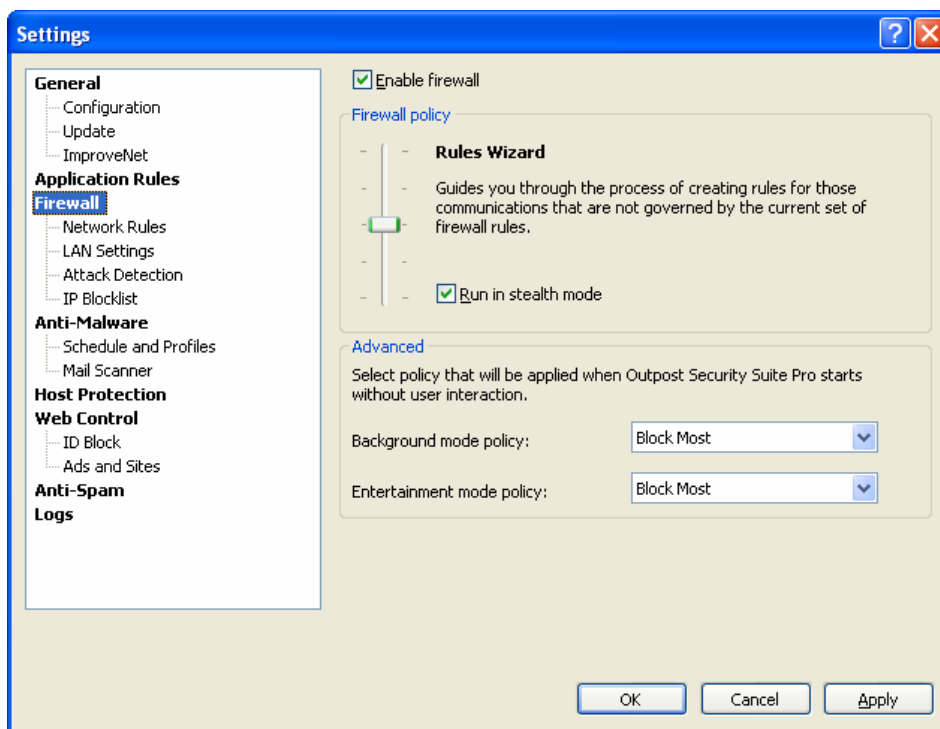
Note:

- If Outpost Security Suite 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 Security Suite 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 Security Suite Pro in stealth mode unless you have some reason not to.

Note:

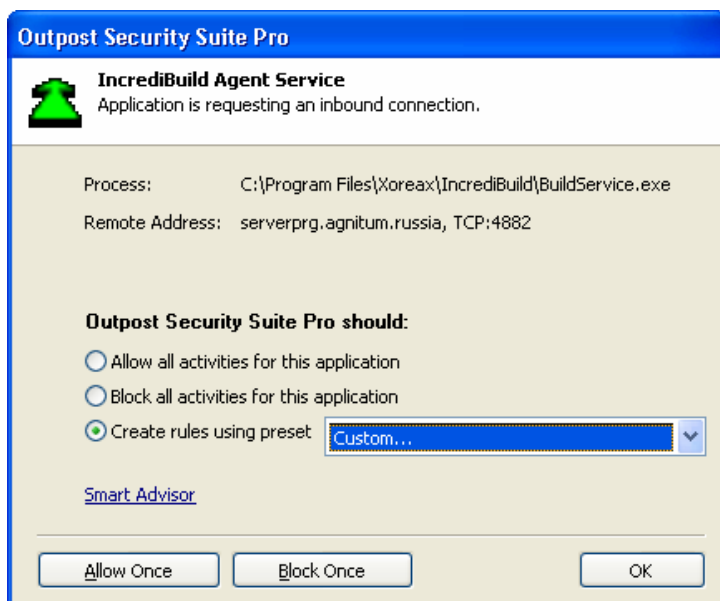
- Because the Rules Wizard policy is not supported when Outpost Security Suite Pro runs in background or Entertainment mode (as these modes do not include interaction with the user), you need to explicitly specify what firewall policy is to be applied when Outpost Security Suite Pro switches to one of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

3.3.1 Running in Rules Wizard Mode

When Outpost Security Suite Pro is first installed, the default policy is **Rules Wizard**. With this policy, Outpost Security Suite 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 Security Suite Pro lets you decide whether an application should be allowed a network connection to a specific address and port.

Outpost Security Suite 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 Security Suite 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 Security Suite 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 Security Suite Pro automatically detects all server addresses and configures the corresponding rules for all the server IP addresses according to the action you specify.

- **Allow Once**

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.

- **Block Once**

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.

Note:

- Rules Wizard is not supported when Outpost Security Suite 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.

3.3.2 Smart Advisor

During its operation, Outpost Security Suite 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 Security Suite 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 Security Suite 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.

3.4 Running in Auto-Learn Mode

To reduce the number of Rules Wizard prompts during the initial stage of Outpost Security Suite 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 Security Suite 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 Security Suite 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 Security Suite Pro system tray icon and select **Enter Auto-Learn Mode**. Specify the period of time you want Outpost Security Suite 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 Security Suite 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.

3.5 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.

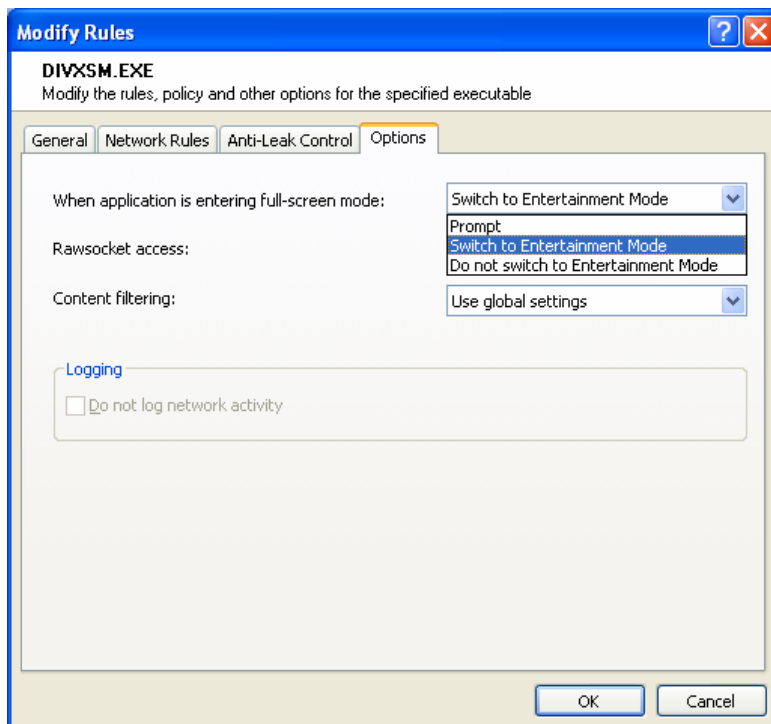
Outpost Security Suite Pro provides a specially designed **Entertainment mode** where protection is active without bothering users with numerous product prompts and alerts. Once the full screen application (a game, media player, etc.) is started, Outpost Security Suite Pro detects this event and suggests 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 and updates are not checked for.

To set Outpost Security Suite 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 Security Suite 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, click **Settings** on the toolbar, select the **Application Rules** tab and double-click the required application. On the **Options** tab, select the necessary action from the **When application is entering full-screen mode** list:



Note:

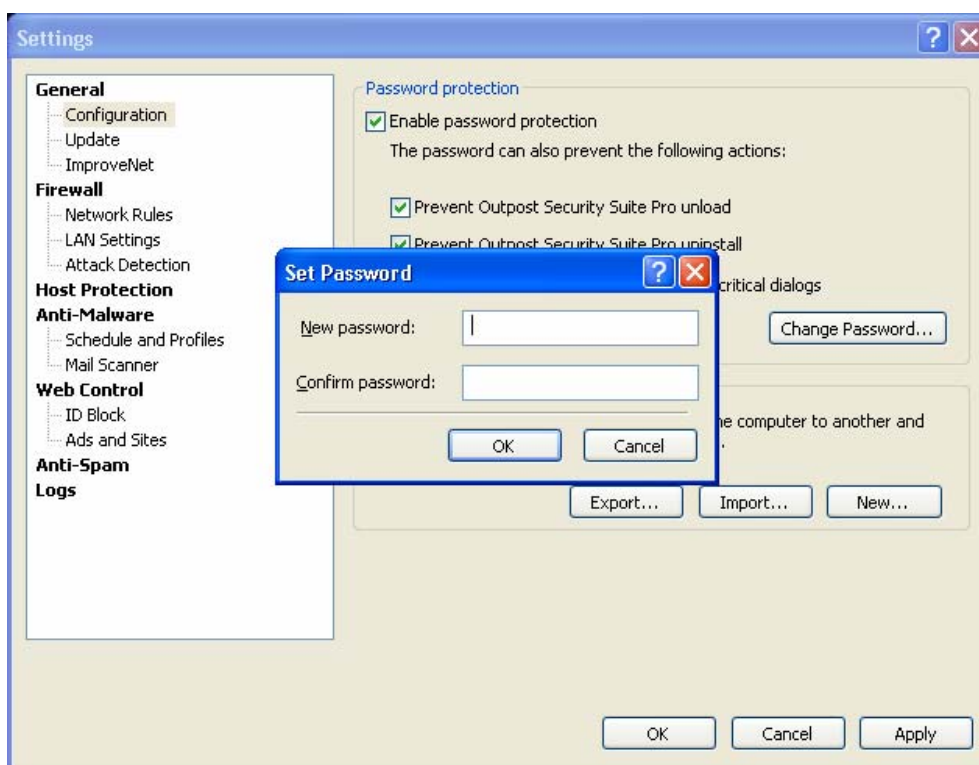
- When operating in background mode, Outpost Security Suite Pro does not need to enter Entertainment mode.

3.6 Protecting Configuration with a Password

Outpost Security Suite 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 Security Suite 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 Security Suite 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 Security Suite 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 Security Suite Pro or even your operating system.

4 Updating Outpost Security Suite 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 antivirus and 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 Security Suite 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 Security Suite 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 Security Suite 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 Security Suite Pro > Update**.

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

Note:

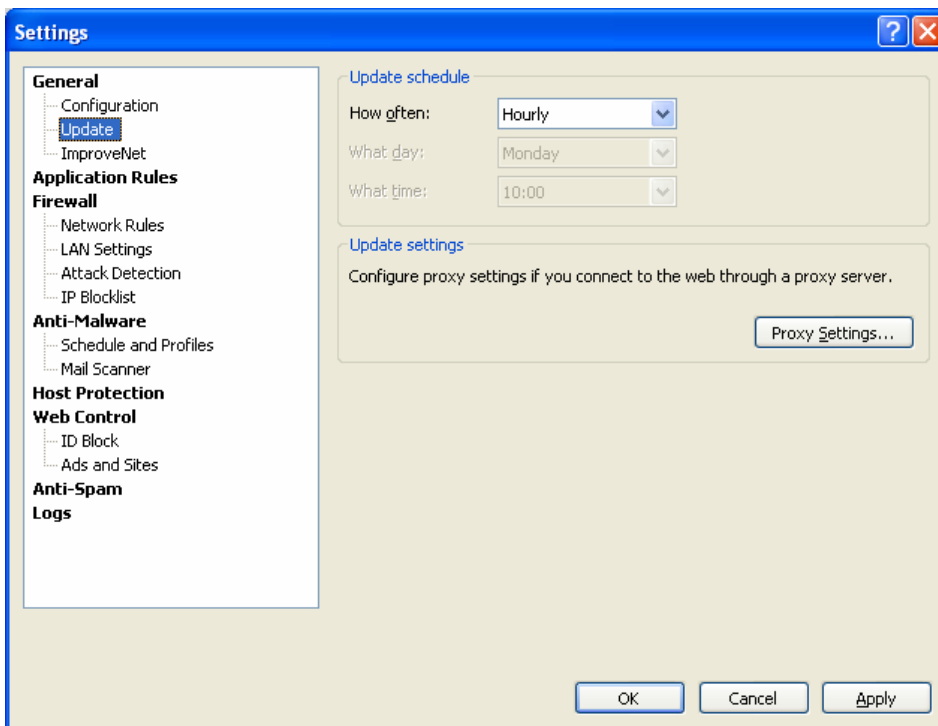
- The current Outpost Security Suite Pro version and modules list are available at the **Update** page of the product settings.

4.1 Configuring Updates

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

Schedule

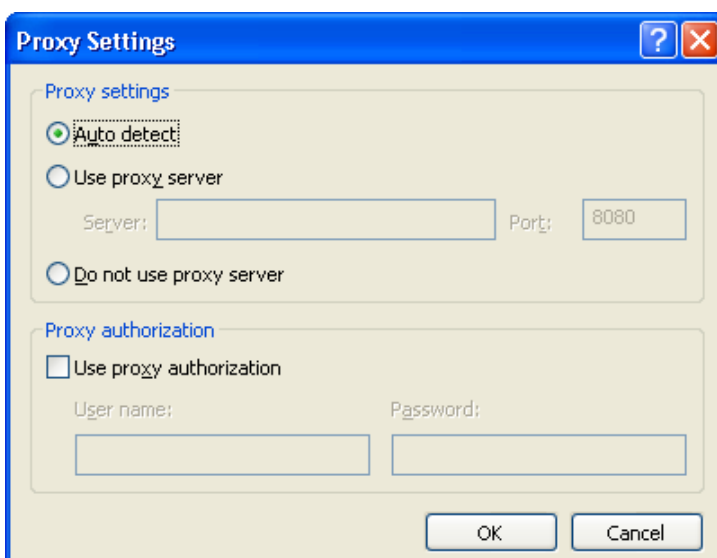
By default, updates take place on an hourly basis, however, you can choose a time when Outpost Security Suite Pro downloads updates on your own. To do this, click the **Settings** button on the toolbar and select the **Update** page:



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. Auto detecting a proxy server is the default option, but 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.

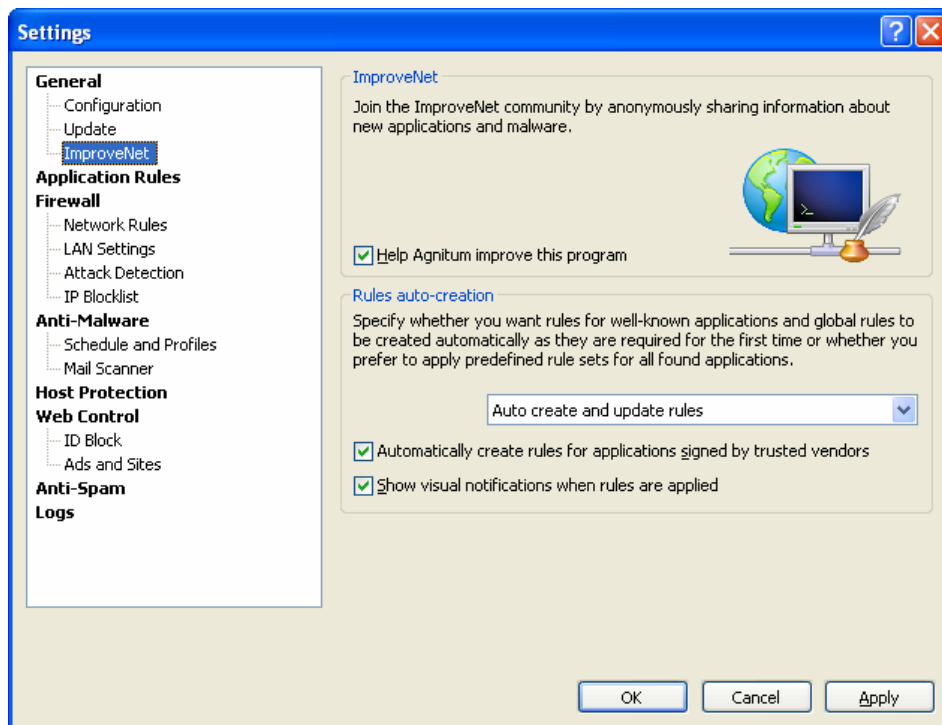
4.2 Agnitum ImproveNet

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 Security Suite 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 Security Suite 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 Security Suite 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 Security Suite 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:



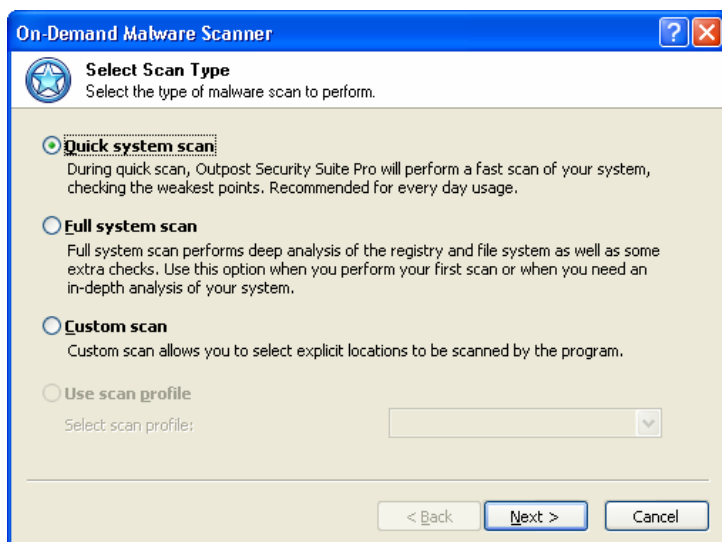
5 Performing a System Scan

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 Security Suite 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.

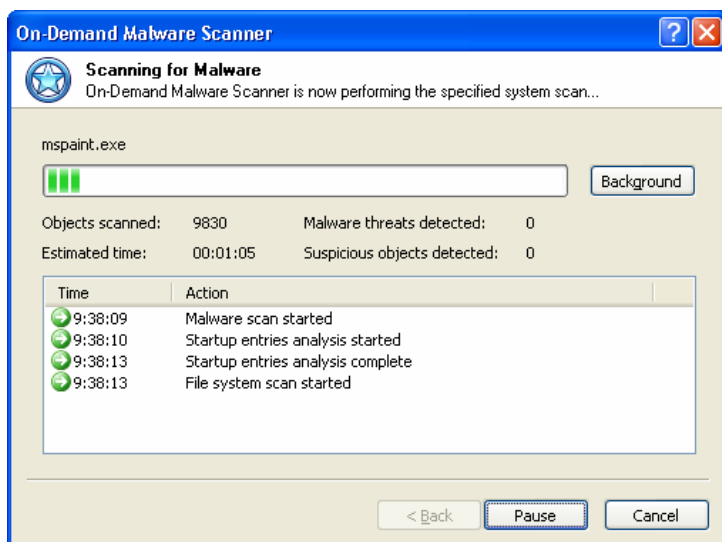
Tip:

- To improve scan performance, you can have Outpost Security Suite 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 Security Suite 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:



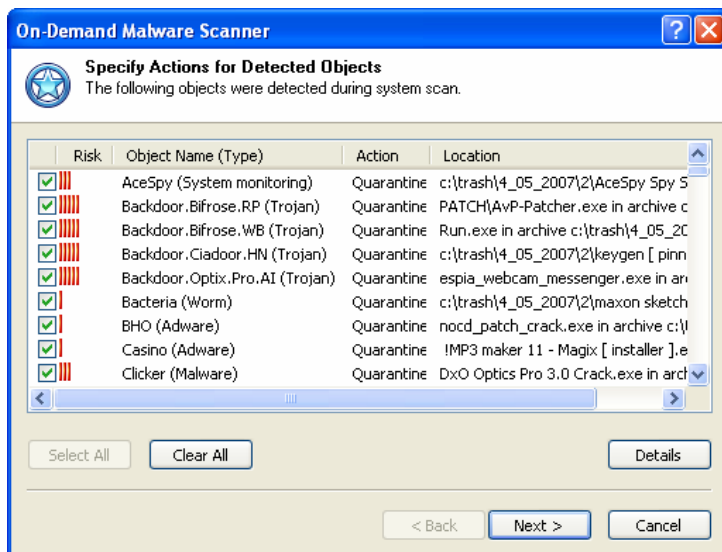
The scanning process can run in background mode. If you want to work with Outpost Security Suite Pro while the scan is underway, click the **Background** button and the wizard will be minimized. To see the full window again, select **Anti-Malware** on the left panel of the main window and click **Show 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 Security Suite 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 Security Suite 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 Security Suite Pro should not scan for malware.

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

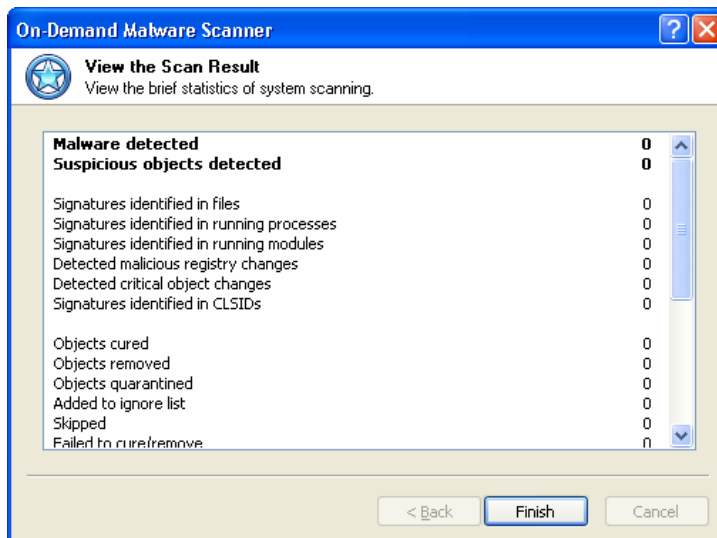
You can later remove items from the exclusions lists using the **Exclusions** button on the **Anti-Malware** dialog page of the product **Settings** window.

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-Malware component detected and removed, open the **Event Viewer** section in the left panel of Outpost Security Suite Pro main window and select the **Anti-Malware** log.

6 Filtering Junk E-Mail

Without a doubt, every Internet user who actively uses e-mail in his everyday activities in the last several years has encountered the problem of unsolicited mass e-mail distribution, known as spam. Especially if he gave his e-mail address to public distribution lists or bulletin boards. The amount of unsolicited information flooding our inboxes is constantly growing. Server-side (run by your Internet Service Provider) anti-spam solutions significantly reduce spam. However, users have no control over server-side solutions. What's worse is the loss of important messages incorrectly labeled as spam and deleted by the system over which the user has no influence.

Agnitum has the solution: the **Anti-Spam** component provides effective filtering of unsolicited incoming mail in a user-specific way. Its remarkable sense of spam is based on the Bayesian statistical method, the most effective known method of automatic statistical filtering of spam. Anti-Spam also provides white lists (people or companies you know and who you want e-mails from) and black lists (known spammers), allowing you to instantly and easily increase spam filtering accuracy.

The filter works independently of the messaging protocol. It ranks e-mail already delivered by the mail client. Not only the content of each letter is considered but also different meta-information like attachments and their size, the time of delivery, "trash" in html-formatted e-mails, etc.; thus making the selection algorithm extremely effective.

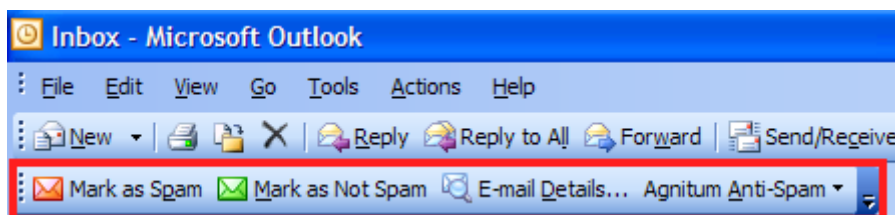
The advantage of Bayesian spam filtering is that it learns on an individual user basis. The spam a user receives is often related to his or her interests. The spam identification of the words mentioned in e-mail a user receives is unique to that user and can evolve over time with corrective training whenever the user sees that the filter incorrectly classified an e-mail. The Bayesian filter assigns spam probability to the words and letters based on the user's own individual traffic.

As a result, Bayesian spam filtering accuracy after some training is often superior to pre-defined rules and it requires minimal input from the user.

6.1 Enabling Spam Filter

After being installed, the Anti-Spam component integrates into your mail client as a simple toolbar providing access to all of its settings.

The Anti-Spam toolbar looks like the following:



To enable or disable spam filtering for either Microsoft Outlook or Microsoft Outlook Express, click **Settings** on the Outpost Security Suite Pro toolbar, select the **Anti-Spam** page and select the corresponding check box.

6.2 Training Anti-Spam Filter

Anti-Spam's Bayesian core is entirely based on statistical information it collects from incoming mail. The actual selection starts after a considerable amount of statistics is collected (the learning stage). Before the learning stage is complete, there are not enough statistics gathered, so the filter cannot rank e-mails. However, when the learning stage is complete, it starts to rank the e-mail you receive according to the spam probabilities of the words contained in your e-mail and automatically marks each message as "spam" or "not spam" according to this ranking.

There is also a non-statistical way that Anti-Spam immediately gets to work marking letters as "not spam". These are e-mails from people on your **Contacts** list, people you write to and your own outgoing

e-mail. These messages are the only ones the filter handles before its training stage is finished. To collect a really valuable knowledge base, Anti-Spam needs some training.

To train it, you can use manual training, automatic training or both methods, whichever you prefer.

6.3 Manual Training

Manual training is based on your use of the **Mark as Spam** and **Mark as Not Spam** buttons on the Anti-Spam toolbar in your mail client. When you receive unsolicited e-mail, don't just delete it; mark it as spam by clicking on the **Mark as Spam** button. Anti-Spam processes the e-mail and learns a bit more what spam looks like, then moves it to the **Spam (detected by Anti-Spam)** folder. Later you will start to see some unsolicited e-mail appearing in the same folder automatically without your interaction. Anti-Spam has learned enough from you to start working independently.

Tip:

- In Microsoft Outlook, you can assign a shortcut to the **Mark as Spam** action in order to make the marking of e-mails as easy as deleting them. (The big difference, of course, is that you're training the filter to do this eventually itself.)

This method is relatively slow because the filter processes e-mails after they have been received. However, after some time the filter will enlarge the knowledge base so he can precisely detect spam without any false positives.

It should be noted that during manual training you don't need to manually mark *all* the incoming messages. But it is *necessary* to mark the ones incorrectly processed by the filter. This is because the filter internally marks all incoming messages (either as "spam" or "not spam") so if the rank it assigns to a message is valid (i.e. it has correctly detected spam or correctly recognized a legitimate message), then the e-mail is already correctly marked and you need do nothing; but if the filter makes a mistake and you don't correct it, then the probability of such errors occurring in the future will increase considerably.

Important:

- During training (especially at the beginning, when the collected statistics are small), it is recommended that you periodically check the junk-mail folder and if you find any e-mail mistakenly detected as spam, mark them as "not spam" using the **Mark as Not Spam** button on the toolbar.

6.4 Automatic Training

The second method of training is "forced". If you already have a sufficient number of both spam and legitimate messages, then you can use the **Anti-Spam Training Wizard** to force the filter to process them to collect statistics for its knowledge base. To start the wizard, click **Agnitum Anti-Spam** on the plug-in toolbar in your mail client and select **Train** on the drop-down menu.

The wizard will first ask you whether you want to append the info to be collected to the existing knowledge base or create a completely new base. After selecting your choice and clicking **Next**, the **Select Spam Folders to Scan** step will be displayed showing all the folders contained in your mailbox and your personal folders (.pst) files, as well as the numbers of messages contained in each folder (in brackets). In the folders tree, select those folders that contain only spam messages. These messages will be processed by the filter to collect statistics of spam words and their probabilities in order to refine the spam filter.

Tip:

- Right-click the folder to select/clear its subfolders.

After designating the folders that contain only spam, click **Next**.

The next step lets you specify folders with only legitimate messages. These will be used to collect statistics for the messages you consider legitimate.

After designating the legitimate folders and clicking **Next**, the wizard starts to process messages in the selected folders. Depending on the number of messages in these folders, this can take some time. When all the messages are processed, the **Finish** button becomes available. Click it to close the wizard. Anti-Spam will then start using his newly created or enhanced knowledge base to filter out spam.

Note:

- To create an effective evaluation database, both "spam" and "not spam" e-mail needs to be processed. It is recommended that the number of messages in one category does not exceed the number of messages in the other category by a factor of ten times or more. When the statistics knowledge base is large enough, such an imbalance does not play a significant role. But for a small knowledge base (for automatic training) or at the first stage of using Anti-Spam (in the case of manual training) the balance between the numbers of processed "spam" and "not spam" messages is very important. For example, if you train the filter with 1000 spam messages and only 10 non-spam ones, the filter will definitely "know" what you consider is spam, but will hardly have any idea about legitimate mail. This will result in errors where the filter will mistakenly rank normal (legitimate) messages as "spam" (false positives).

Tip:

- If you consider all messages that are sent off from your computer as legitimate (a reasonable assumption), you can use these to train Anti-Spam. To set the filter to mark all outgoing messages as "not spam", select the **Train Anti-Spam on my outgoing e-mail also** check box on the **General** tab of Anti-Spam settings.

7 Uninstalling Outpost Security Suite Pro

To uninstall Outpost Security Suite Pro:

1. Right-click the Outpost Security Suite 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 Security Suite 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.

8 Troubleshooting

If you need assistance in working with Outpost Security Suite 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 Ltd. is a software development company committed to delivering and supporting high quality security software products. Agnitum offers two headline products - Outpost Security Suite Pro PRO, securing personal and family desktops, and Outpost Network Security, ensuring a reliable endpoint protection and performance of the corporate network. Agnitum delivers computer security solutions to large enterprises, small and medium businesses, as well as home PC users.

North America Sales Office:

130 El Bosque Ave.
San Jose, CA 95134

HQ address:

Acropoleos Avenue
8 Mabella Court
Nicosia, Cyprus