



OUTPOSTPRO

SECURITY SUITE

User Guide

Abstract

This is the complete and detailed reference to the Outpost Security Suite Pro software.

For an entry-level guide, please see the Getting Started guide.

To get help while using the product, press the F1 button on the keyboard.

You can get additional information about the product at www.agnitum.com.

Please note that further versions of Outpost Security Suite Pro may have other options and dialogs than the 2008 version.

Table of contents

| | |
|--|-----------|
| 1 Welcome to Outpost Security Suite Pro | 5 |
| 1.1 System Requirements..... | 6 |
| 1.2 Installing Outpost Security Suite Pro..... | 6 |
| 1.3 Registering Outpost Security Suite Pro..... | 13 |
| 2 User Interface and Controls Basics | 15 |
| 2.1 The Toolbar..... | 15 |
| 2.2 Left and Information Panels..... | 16 |
| 2.3 System Tray Icon..... | 17 |
| 2.4 Interface Language..... | 19 |
| 3 Basic Configuration | 20 |
| 3.1 Starting and Stopping Protection..... | 20 |
| 3.2 Creating a New Configuration..... | 23 |
| 3.3 Protecting Configuration with a Password..... | 26 |
| 4 Updating Outpost Security Suite Pro | 28 |
| 4.1 Configuring Updates..... | 28 |
| 4.2 Agnitum ImproveNet..... | 30 |
| 5 Managing network connections | 32 |
| 5.1 Selecting the Firewall Policy..... | 32 |
| 5.1.1 Running in Rules Wizard Mode..... | 34 |
| 5.1.2 Running in Auto-Learn Mode..... | 35 |
| 5.1.3 Running in Entertainment Mode..... | 36 |
| 5.1.4 Smart Advisor..... | 37 |
| 5.2 Configuring Local Network Settings..... | 38 |
| 5.2.1 Detecting a Local Area Network..... | 38 |
| 5.2.2 Specifying LAN Access Levels..... | 40 |
| 5.3 Managing Applications Network Access..... | 40 |
| 5.3.1 Managing List of Applications..... | 41 |
| 5.3.2 Managing Rules for Applications..... | 42 |
| 5.4 Managing Global System Network Activity..... | 44 |
| 5.4.1 Managing Global Rules..... | 45 |
| 5.4.2 Managing Low-Level System Rules..... | 46 |
| 5.4.3 Controlling ICMP Protocol Activity..... | 46 |
| 6 Preventing Network Attacks | 48 |
| 6.1 Specifying Attack Detection Level..... | 48 |
| 6.2 Protecting from Ethernet Attacks..... | 49 |
| 6.3 Port Scanning..... | 50 |
| 6.4 Attacks List..... | 52 |
| 6.5 Specifying Trusted Hosts and Ports..... | 53 |
| 7 Protecting a Host from Malicious Process Activity | 55 |
| 7.1 Setting Local Security Level..... | 55 |
| 7.2 Controlling Penetration Techniques..... | 56 |
| 7.3 Controlling Application Components..... | 57 |
| 7.4 Controlling Critical System Objects..... | 60 |
| 8 Protecting against Malware | 61 |
| 8.1 Performing a System Scan..... | 61 |
| 8.1.1 Selecting Scan Type..... | 61 |
| 8.1.2 Selecting Objects to Scan..... | 62 |
| 8.1.3 Scanning Specified Locations..... | 63 |
| 8.1.4 Removing Detected Malware..... | 64 |
| 8.1.5 Viewing Scan Results..... | 65 |
| 8.2 Real-Time Protection..... | 66 |
| 8.3 Scanning Mail Attachments..... | 67 |
| 8.4 Malware Quarantine..... | 69 |

| | |
|---|-----------|
| 8.5 Scheduling System Scan | 69 |
| 9 Controlling Online Activities | 71 |
| 9.1 Setting Web Control Level..... | 71 |
| 9.2 Advertisement Blocking..... | 73 |
| 9.3 Specifying Exclusions..... | 74 |
| 9.4 Site Blacklist | 75 |
| 9.5 Blocking Private Data Transfers | 75 |
| 10 Filtering Junk E-Mail | 77 |
| 10.1 Enabling Spam Filter..... | 77 |
| 10.2 Training Anti-Spam Filter..... | 77 |
| 10.2.1 Manual Training | 78 |
| 10.2.2 Automatic Training | 78 |
| 10.2.3 How Does the Bayesian Filter Work? | 80 |
| 10.3 Scanning Mail Folders | 80 |
| 10.4 Setting the Filtering Level..... | 81 |
| 10.5 Specifying White and Black Lists | 83 |
| 10.6 Specifying Additional Settings..... | 84 |
| 11 Protecting Internal Components | 87 |
| 12 Uninstalling Outpost Security Suite Pro | 88 |
| 13 Tracking System Activity | 89 |
| 13.1 Logging Level..... | 90 |
| 14 Appendix | 91 |
| 14.1 Troubleshooting | 91 |
| 14.2 Understanding Penetration Techniques..... | 91 |
| 14.3 Using Macro Addresses | 93 |
| About Agnitum | 95 |

1 Welcome to Outpost Security Suite Pro!

Proactive Protection for Intelligent Internet Users

Today's Internet requires a whole new approach to security. Almost everything is interconnected and taking place in real time. And that includes threats. To be effective, security software must be constantly alert for new forms of deviousness.

New types of threats require new forms of protection. Mass-distribution of viruses and worms is giving way to profit-driven attacks designed to steal identities, money, and other valuable electronic commodities through phishing and social engineering.

To fully protect against these new risks, an effective security solution must deploy a multi-layered approach, providing proactive, behavior-based blocking as well as the more traditional database-driven signature detections. It must also be easy to use, because if it's not, it won't *be* used.

Agnitum is happy to introduce a brand new security product – Outpost Security Suite Pro. Being a successor of the acclaimed Outpost Firewall Pro, Outpost Security Suite Pro combines the best of both approaches in a single integrated product that delivers customized protection and total reliability. Outpost Security Suite Pro protects your electronic jewels 24 hours a day, seven days a week – no matter what you're doing.

Key Benefits

- The firewall controls your computer's connections with other PCs by blocking hackers and preventing local and remote unauthorized network access. The firewall controls application inbound and outbound Internet access, as well as stops malware from communicating to or from your PC.
- Host Protection monitors program behaviors and interactions in order to proactively defend against unauthorized activity. It also blocks Trojans, spyware, and all kinds of sophisticated hacking techniques that try to compromise your system's security or steal your data.
- Outpost Security Suite Pro uses specialized techniques to ensure that its own protection cannot be disabled by specific types of malware that were designed to do just that.
- The suite's lightweight yet effective malware scanner detects and quarantines or directly removes viruses, spyware and other malicious software automatically. The resident on-access monitor is constantly on guard against malware that's lying idle or being activated, yet has little or no impact on system performance.
- The anti-spam engine keeps your inbox free of junk email. You can train it to recognize and use your personal definition of spam, so it becomes more efficient and an even greater time saver the longer it's used.
- The versatile Web Control module safeguards you against the Internet's darker side. It steers you away from websites infected with drive-by downloads, prevents the inadvertent disclosure of personal information, limits your exposure to potentially unsafe web properties, and keeps your identity private.
- Powerful, easy to use protection offers extensive assistance for beginners in making the best use of the product, while advanced users will welcome the wealth of control options and customizable settings they can use to customize their own configurations.

This online help provides information on Outpost Security Suite Pro's interface, settings, and functionality. For more information about features and for additional documentation, please visit <http://www.agnitum.com/products/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;
- Windows Mail.

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.

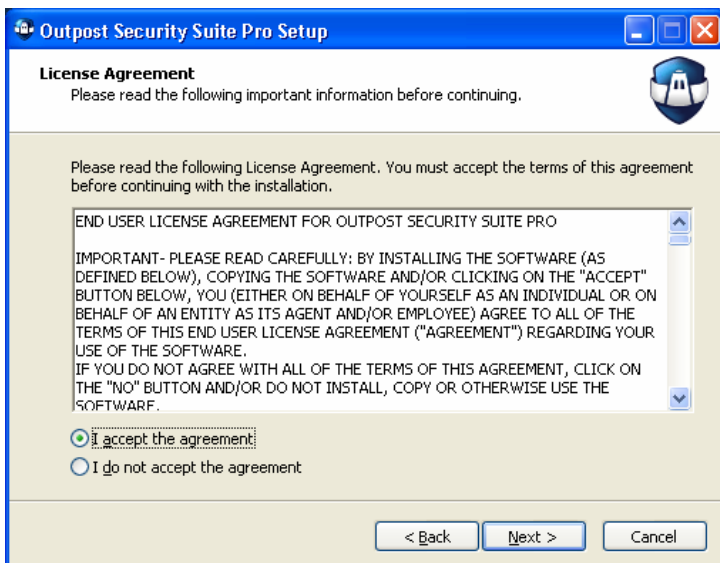


Choose the language for Outpost Security Suite Pro interface and click **OK**. Setup will display the **Welcome** dialog presenting basic features of the product:

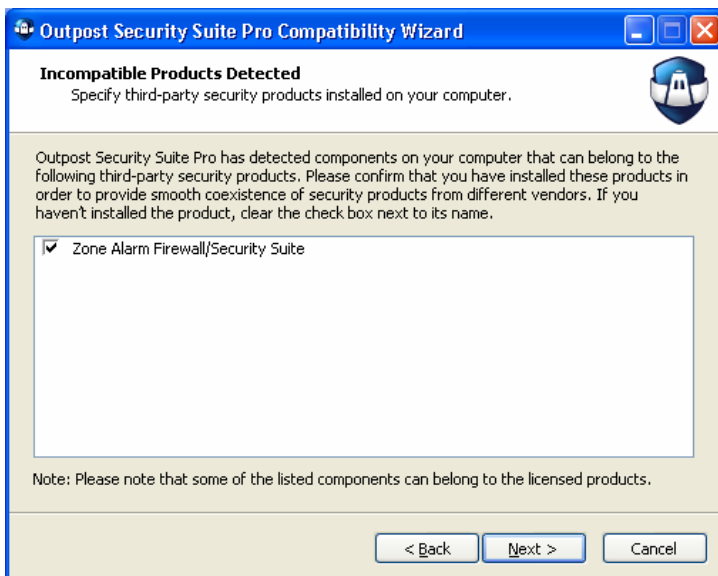


After clicking the **Next** button you will be asked to accept the License Agreement to use the **Outpost Security Suite Pro**.

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:



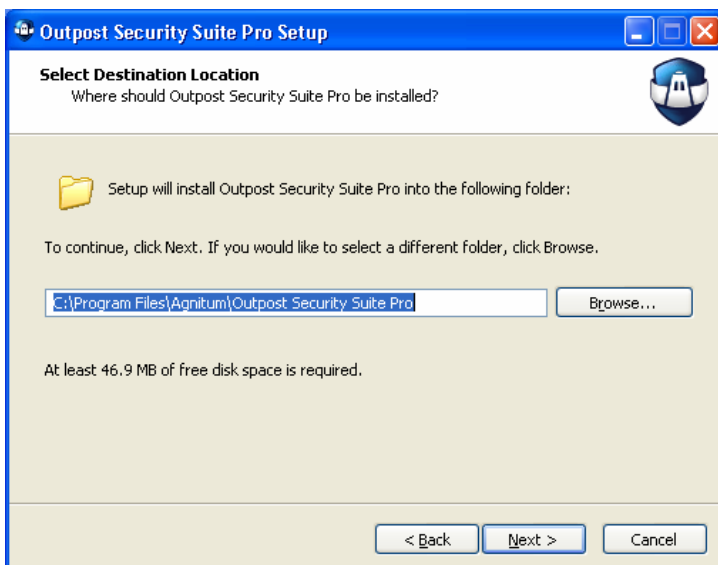
In case you have not removed any third-party security software, the setup wizard will display a prompt pointing at detecting incompatible software:



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

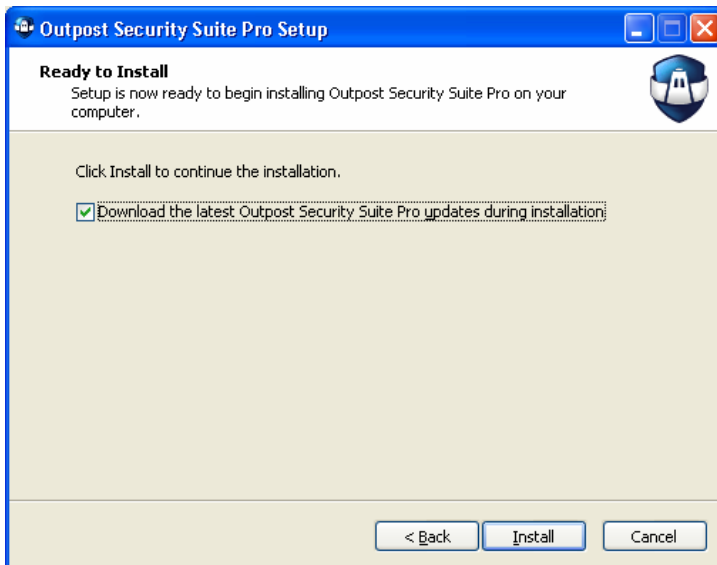
On detecting *a partly compatible product* the wizard will offer you one of the possible options to apply to the product.

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.

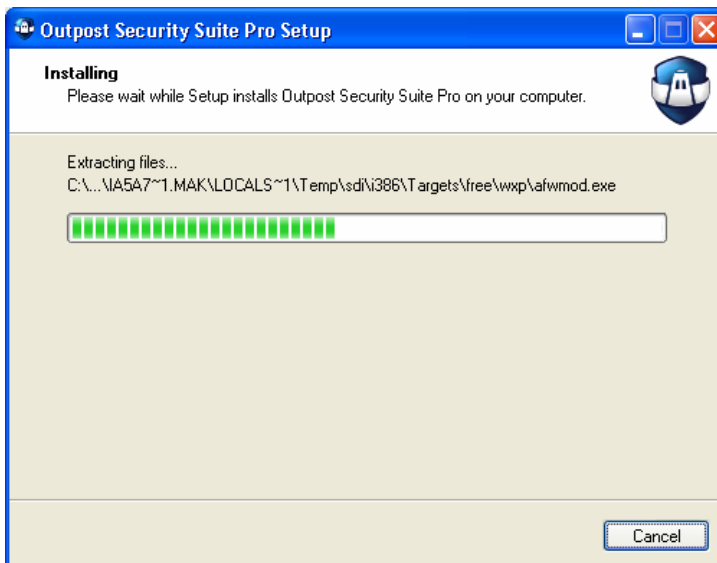
If you want to change the default file location, click **Browse**. Select the folder or create your own one and click **OK**. Click **Next** to proceed to the last step before actual installation:



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:

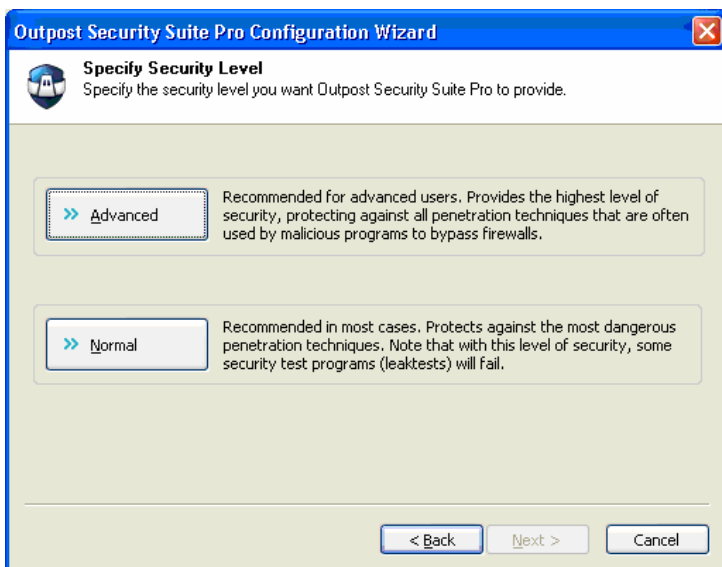


After the installation is finished, the **Configuration Wizard** will help you create a new configuration or import the previous if you install the product over an earlier version:



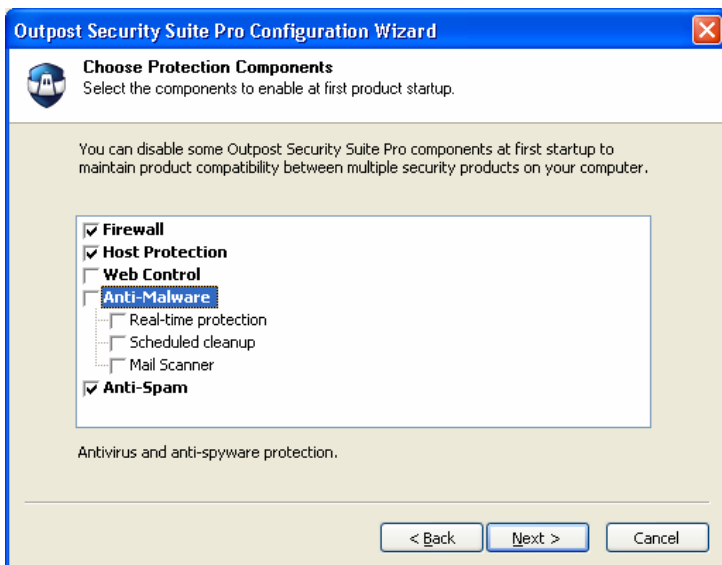
On importing a previous configuration the system will automatically copy saved settings of the earlier version, after which you will need to reboot the computer to complete Outpost Security Suite Pro installation.

On creating a new configuration the setup wizard will offer you to select a necessary security level:

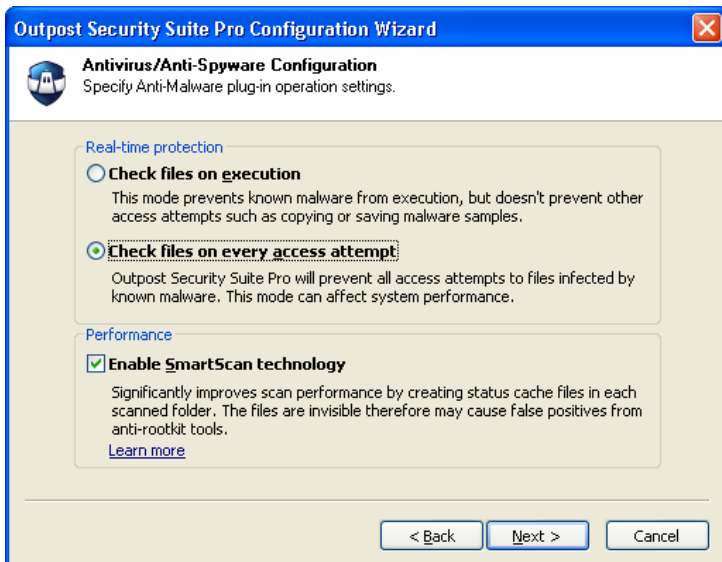


Advanced security provides the highest level of security and protects against all penetration techniques that are often used by malicious programs to bypass firewalls. **Normal** security protects against the most dangerous penetration techniques. It decreases a number of product prompts for users to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

With the next step you will be able to enable the product components according to your needs:



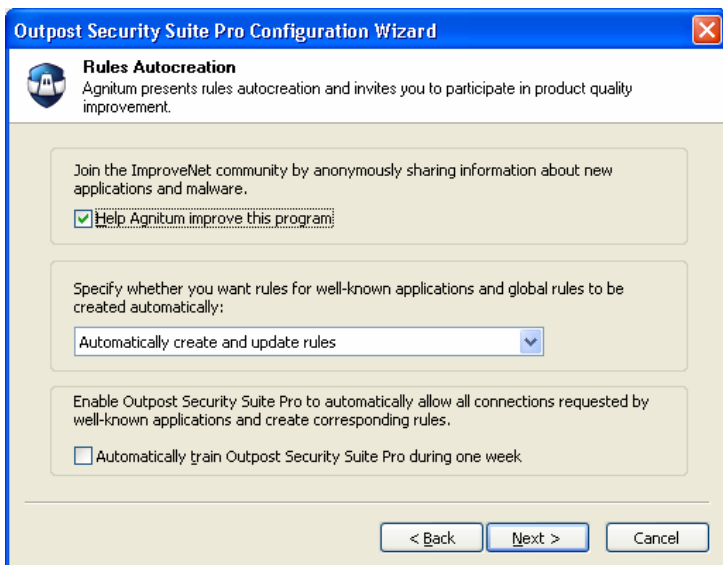
With the next step you will be able to set Antivirus and Antispyware configuration:



If you do not want malware programs on your computer to launch, select **Check files on execution**. If you want Outpost Security Suite Pro to prevent all other access attempts to files that are infected with known malware, such as copying or saving a program's copies, select **Check files on every access attempt**. Note that checking files on every access attempt does slow system performance.

You could increase scan performance by selecting the **Enable SmartScan technology** check box. While using the SmartScan technology, Outpost Security Suite Pro creates status cache files in every scanned folder. These files are invisible, so may cause false positives from anti-rootkit tools.

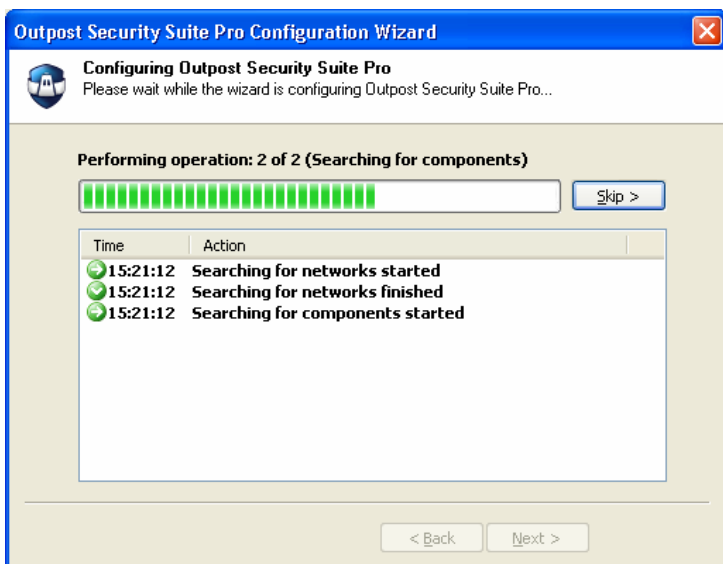
Click **Next** to proceed to the **Rules Autocreation** step, which lets you to enable rules autocreation, so global rules and rules for well-known applications are created automatically when they first request an action (for example, network access or process memory modification). If you do not want 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 Security Suite Pro during one week** option allows product to create necessary rules automatically.

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. For details, see Agnitum ImproveNet.

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

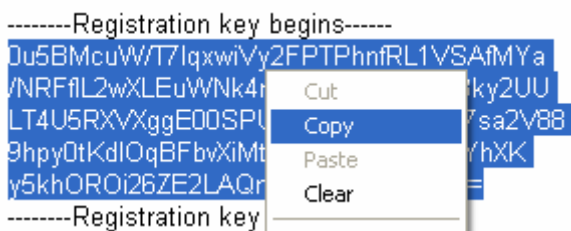
Outpost Security Suite Pro is available for your free evaluation. You are entitled to evaluate the software during the trial period with no obligation to pay. After the trial period, if you decide to keep the software and would like to receive free annual updates, you must register your copy with us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

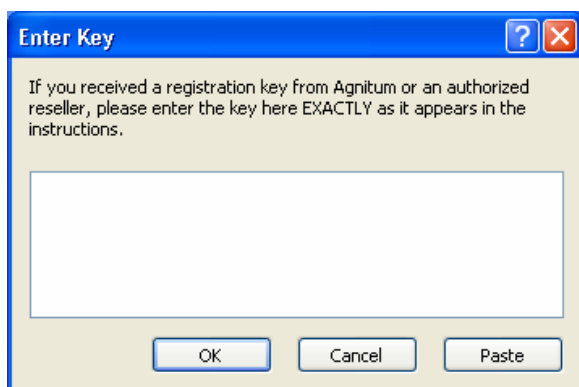
If you downloaded your copy from Agnitum's web site, to register your version, you need to purchase your registration key. Follow the instructions on the page <http://www.agnitum.ru/purchase/outpost/>, and you will receive your registration key by e-mail.

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.ru/purchase/renewal/index.php>.

Note:

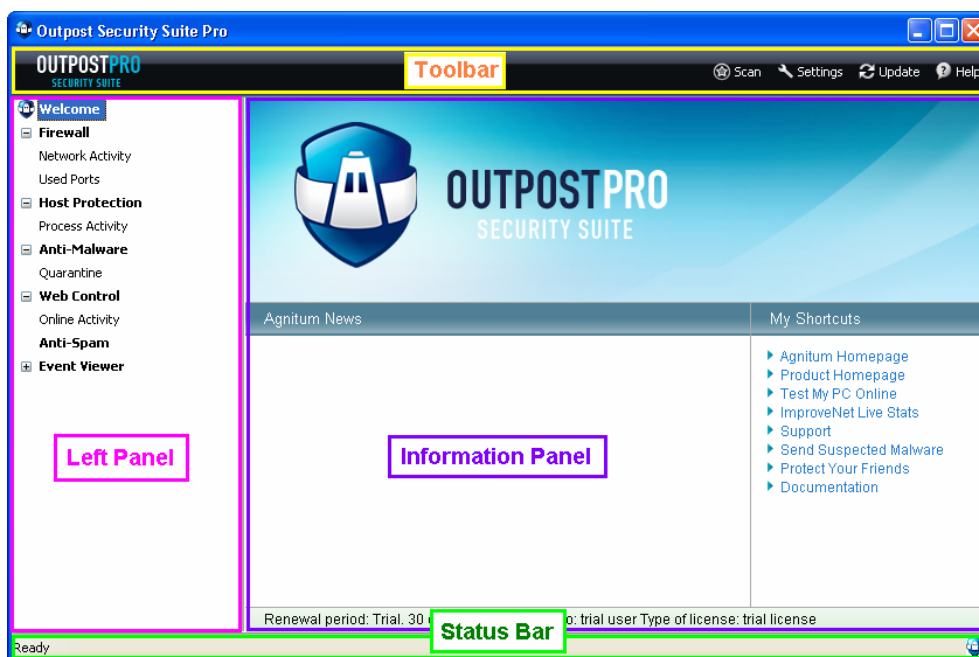
- Outpost Firewall Pro and Outpost Security Suite Pro are independent products and their registration keys are not interchangeable. It means that Outpost Firewall Pro registration key is not applicable to Outpost Security Suite Pro and visa versa. Please, be sure you are entering the correct registration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

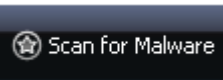


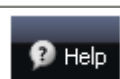
The status bar is at the bottom of the main window. It is used to display the Outpost Security Suite Pro's current state.

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:

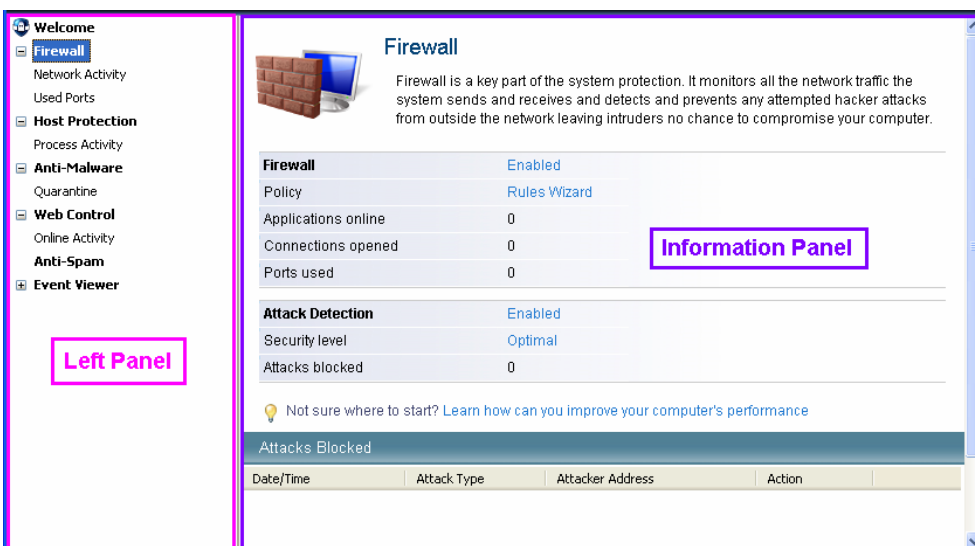
These are the buttons found on the toolbar:

| 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:



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 displays 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. See [Managing Network Connections](#) for details.

- **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. See [Protecting a Host from Malicious Process Activity](#) for details.

- **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. See [Protecting against Malware](#) for details.

- **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. See [Controlling Online Activities](#) for details.


- **Anti-Spam**

Displays general statistics for all e-mail messages marked as spam or probable spam. For information about the **Anti-Spam** component, see [Filtering Junk E-Mail](#).

- **Event Viewer**

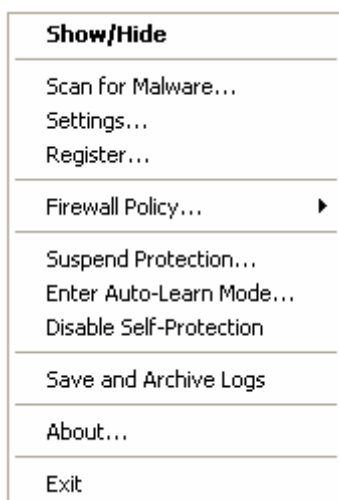
Displays detailed statistics for all past system and product activities by category. For details, see [Tracking System Activity](#).

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:

- **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.

- **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.

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

Disables (enables) Outpost Security Suite Pro [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.

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

Disables (enables) Outpost Security Suite Pro [self-protection](#).

- **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. For details, see [Logging Level](#).

- **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.

- **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.

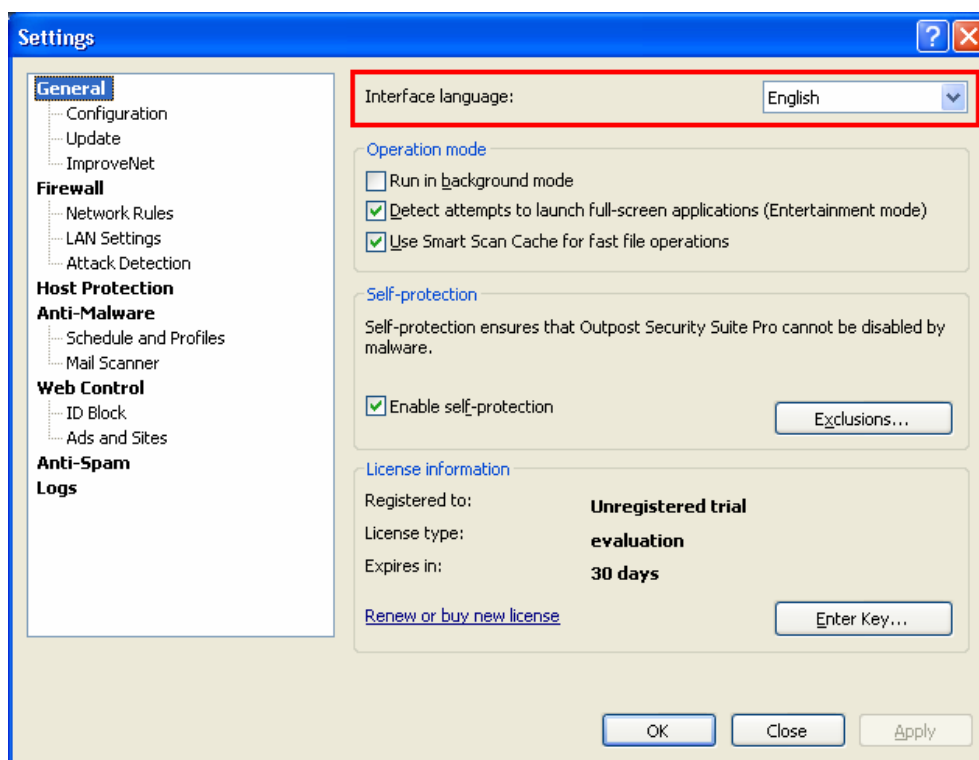
Note:

- 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 **Outpost Security Suite Pro 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.

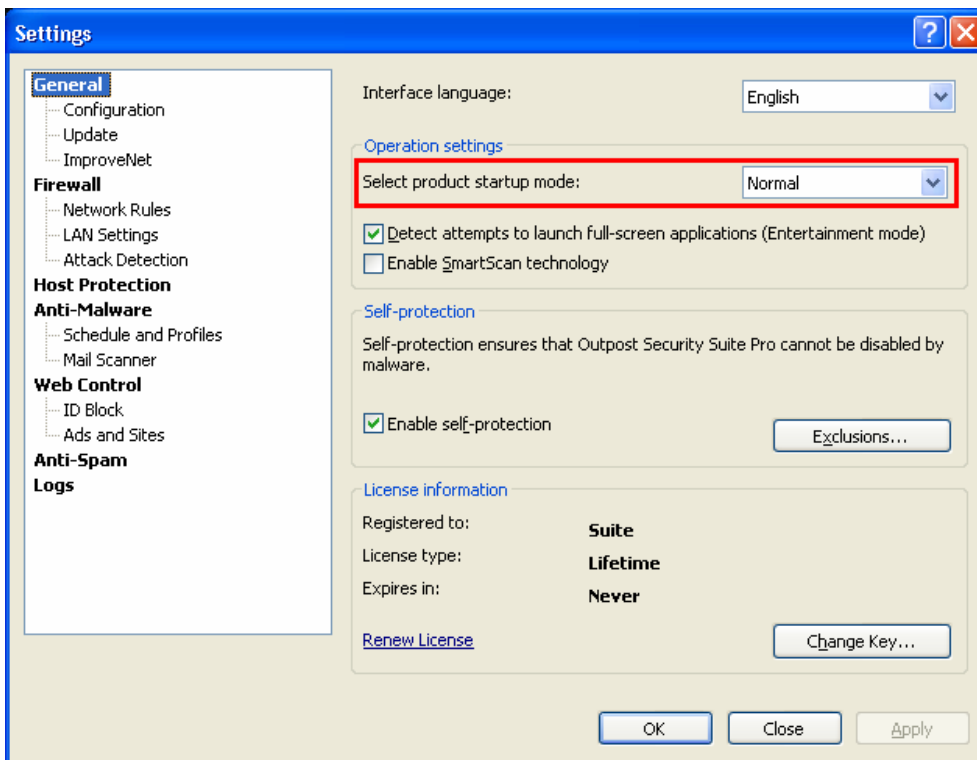
To completely stop Outpost Security Suite Pro so it no longer protects your system, right-click the Suite's icon in the system tray, click **Exit**, select **Exit Outpost Security Suite Pro and shutdown service** from the list and click **OK**.

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:

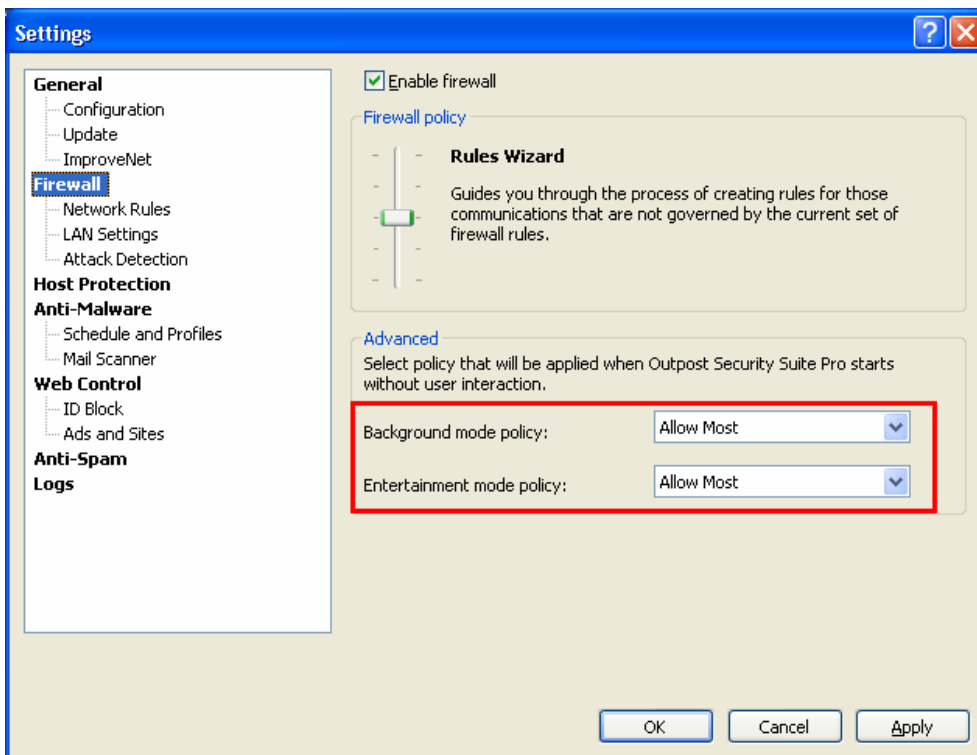
- **Normal** - the default mode. Loads Outpost Security Suite Pro automatically when you turn on your computer and displays its icon in the system tray.
- **Background** - when in background startup mode, Outpost Security Suite Pro runs invisibly without displaying its system tray icon or any of its 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:



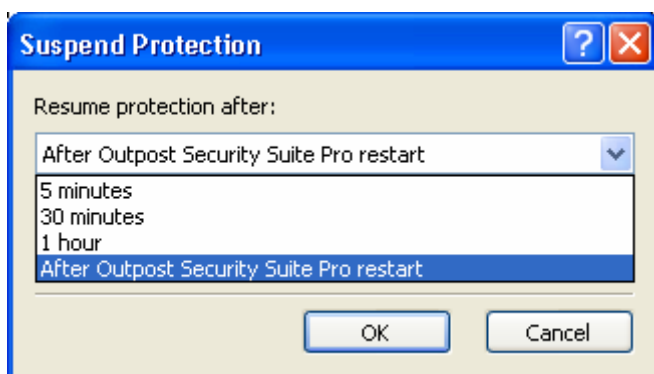
You can manually start Outpost Security Suite Pro at any time by selecting **Start > All Programs > Agnitum > Outpost Security Suite Pro** and clicking **Outpost Security Suite Pro**. To close Outpost Security Suite Pro's GUI and switch to background mode, right-click the suite's icon in the system tray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

Suspending protection

Outpost Security Suite Pro allows you to temporarily suspend its protection for a specified period of time. This is very convenient if you do not want to unload the product completely, yet need to disable protection for a short period to avoid excess pop-up dialogs, for example, while installing trusted third-party software, testing an application, or performing some low-level activity that might be considered suspicious. When you suspend protection, the product stops controlling activities; on resuming protection, it applies the configuration used before suspension.

To suspend protection, right-click the suite's icon in the system tray and click **Suspend Protection**. You will be asked for the duration you'd like the suite to be suspended, after which the protection will be resumed. Select the period and click **OK** to suspend:



You can resume protection at any time during the duration of suspension by right-clicking the suite's icon and selecting **Resume Protection**.

Disabling Outpost Security Suite Pro's components

You can also stop Outpost Security Suite Pro's components separately instead of stopping or suspending the entire suite, if you do not need specific components functioning:

- To disable the **firewall**, click **Settings** on the toolbar, select the **Firewall** page and clear the **Enable firewall** check box. Disabling the firewall also disables the attack detection functionality. See [Managing Network Connections](#) for details.
- To disable only the **Attack Detection** component, click **Settings** on the toolbar, select the **Firewall > Attack Detection** page and clear the **Enable Attack Detection** check box. See [Preventing Network Attacks](#) for details.
- To disable **Host Protection**, click **Settings** on the toolbar, select the **Host Protection** page and clear the **Enable Host Protection** check box. See [Protecting from Malicious Process Activity](#) for details.
- To disable the **real-time malware protection**, click **Settings** on the toolbar, select the **Anti-Malware** page and clear the **Enable real-time protection** check box. See [Real-Time Protection](#) for details.
- To disable the **mail scanner**, click **Settings** on the toolbar, select the **Anti-Malware > Mail Scanner** page and select **Do not scan mail**. See [Scanning Mail Attachments](#) for details.

- To disable **Anti-Spam**, click **Settings** on the toolbar, select the **Anti-Spam** page and clear the **Enable spam filtering in Outlook (Outlook Express)** check box depending on your mail client. See [Enabling Spam Filter](#) for details.
- To disable **Web Control**, click **Settings** on the toolbar, select the **Web Control** page and clear the **Enable Web Control** check box. See [Controlling Online Activities](#) for details.
- To disable Outpost Security Suite Pro **self-protection**, click **Settings** on the toolbar and clear the **Enable self-protection** check box. See [Protecting Internal Components](#) for details.

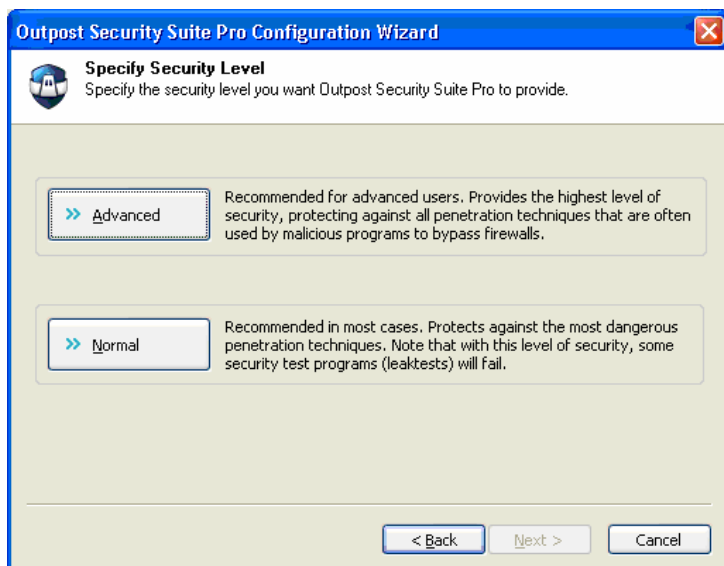
Note:

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

3.2 Creating a New Configuration

The exact state of Outpost Security Suite Pro at any moment of time is represented by all of its settings, which include: policy, components security levels, application and global rules, LAN settings, exclusion lists, etc. The totality of these settings is called the *configuration*. The first configuration is created during installation. You can always modify any of the settings and even create different configurations for different activities. This allows for separate configurations for each computer user, such as: configurations to prevent children from accessing unacceptable sites, from playing online games or chatting if they use their parent's computer. This makes it easy to transfer configuration settings from one computer to another and easy to back up your configurations. Switching between configurations is very quick.

To create a new configuration, click **Settings > Configuration > New**. The product configuration is performed automatically with the help of the **Configuration Wizard**:



The first step lets you select the local security level you'd prefer. The following levels are available (for details, see [Protecting from Malicious Process Activity](#)):

- **Advanced.** Provides the best protection against all penetration techniques that are most often used by malicious software to bypass firewalls. Having selected this level, you will get a lot of product prompts that require your response; therefore it is recommended for advanced users.
- **Normal.** Ensures protection only against the more dangerous techniques, has a reduced number of product prompts that require your response and is recommended for most cases. However, if **Normal** security level is selected, some of the more exotic security test programs (leaktests) will fail.

Click the desired security level to proceed. With the next step you will be able to enable the product components according to your needs:



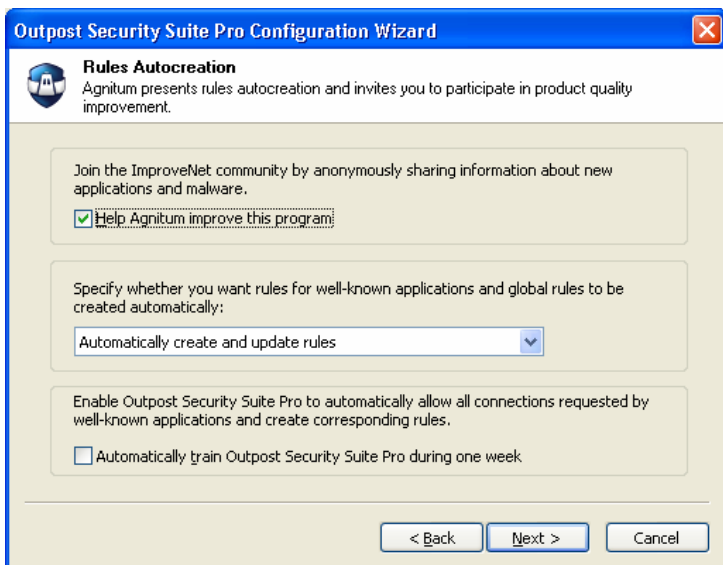
The next step lets you configure the real-time malware protection operation mode:



If you do not want malware programs on your computer to launch, select **Check files on execution**. If you want Outpost Security Suite Pro to prevent all other access attempts to files that are infected with known malware, such as copying or saving a program's copies, select **Check files on every access attempt**. Note that checking files on every access attempt does slow system performance.

You could increase scan performance by selecting the **Enable SmartScan technology** check box. While using the SmartScan technology, Outpost Security Suite Pro creates status cache files in every scanned folder. These files are invisible, so may cause false positives from anti-rootkit tools.

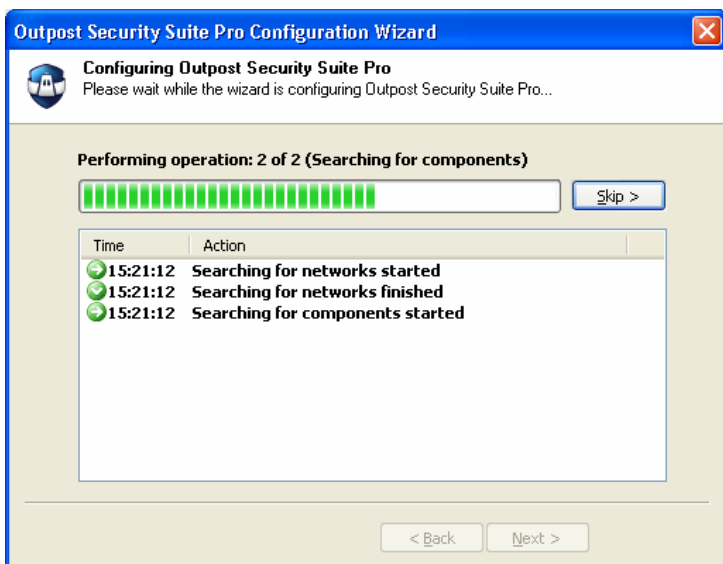
Click **Next** to proceed to the **Rules Autocreation** step, which lets you to enable rules autocreation, so global rules and rules for well-known applications are created automatically when they first request an action (for example, network access or process memory modification):



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

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. See [Agnitum ImproveNet](#) for details.

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. By default the created configuration is called **configurationN.cfg** (where N is an increasing number) and is saved in the Outpost Security Suite Pro installation folder.

You can create several configurations by changing specific settings and giving each configuration a different name using the **Export** command. To switch to another configuration, click **Import** and browse to the configuration file.

A configuration can be protected from being modified or swapped by specifying a password. For details see [Protecting Configuration with a Password](#).

Note:

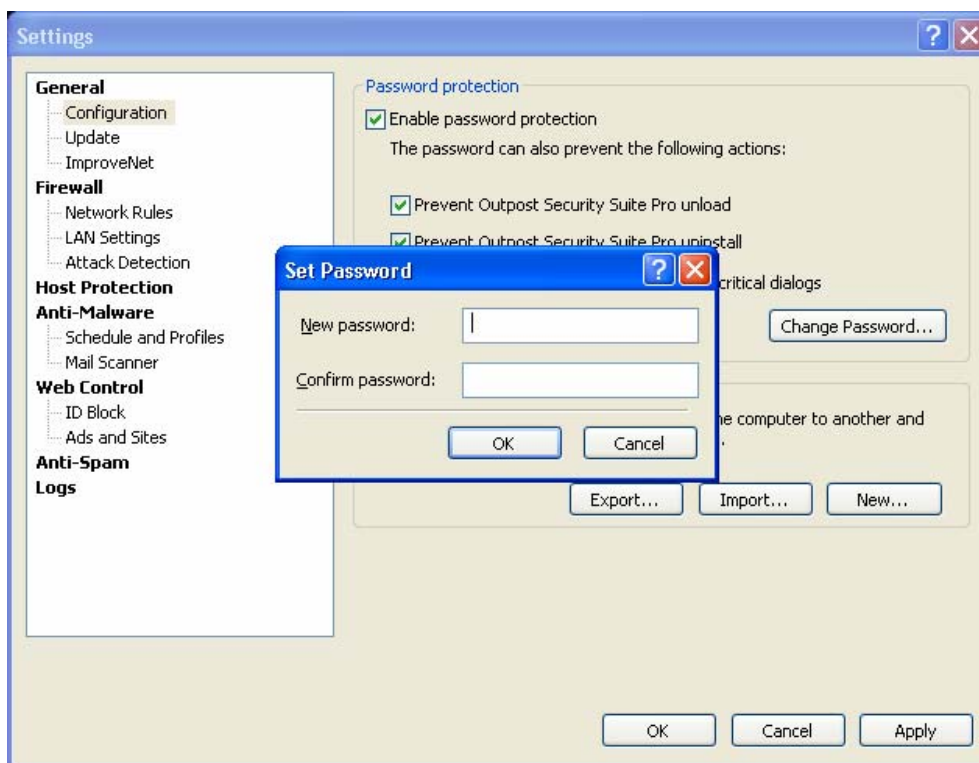
- When exiting Outpost Security Suite Pro, the configuration file that is currently in use is saved so it will be automatically loaded the next time Outpost Security Suite Pro is started.

3.3 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**.

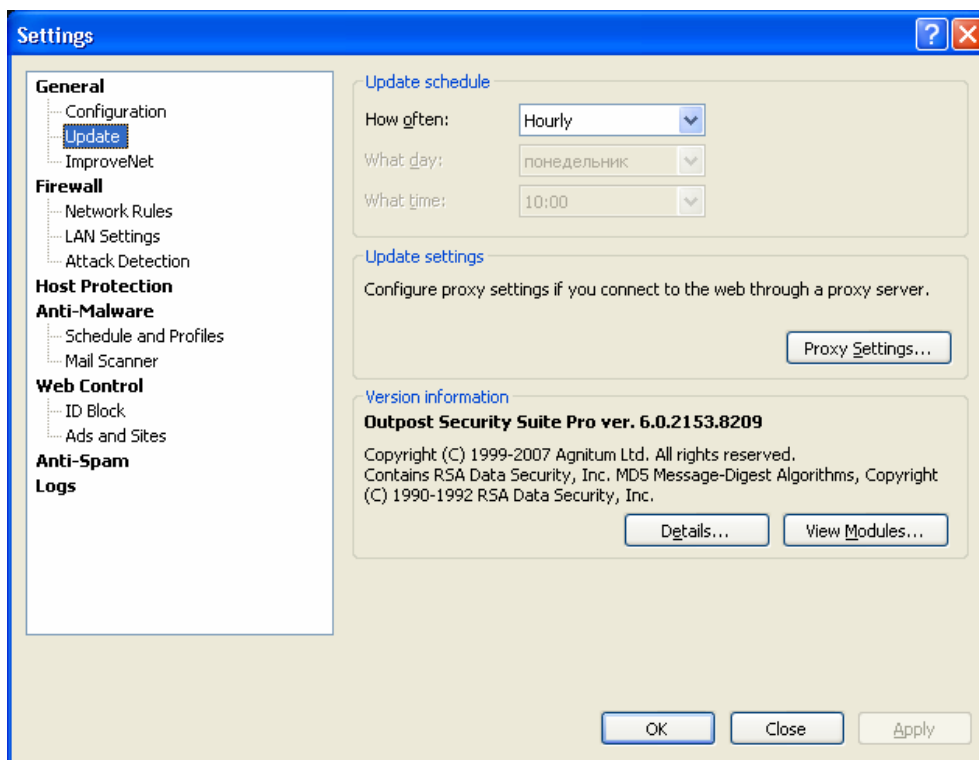
Agnitum lets you change the regular [updates schedule](#) and suggests that you personally may want to help in updating Outpost Security Suite Pro's rules by participating in a completely free [Agnitum ImproveNet](#) program.

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:



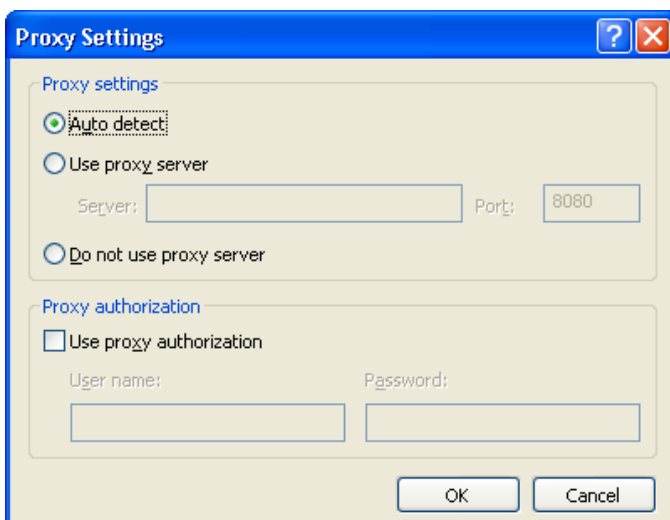
Schedule

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.

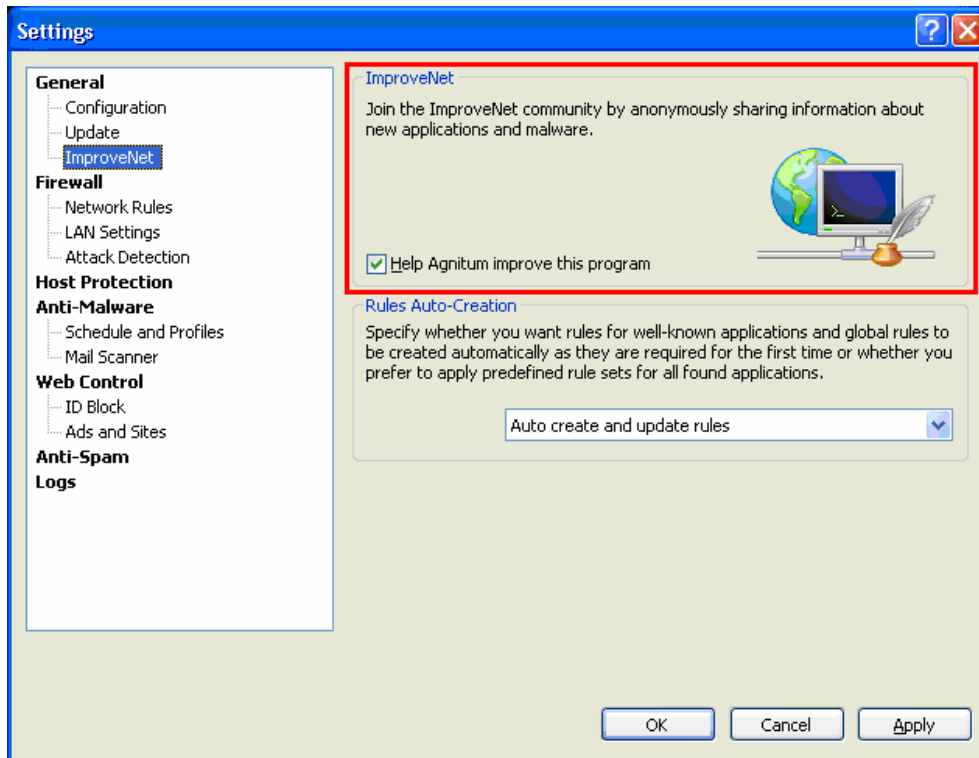
4.2 Agnitum ImproveNet

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:

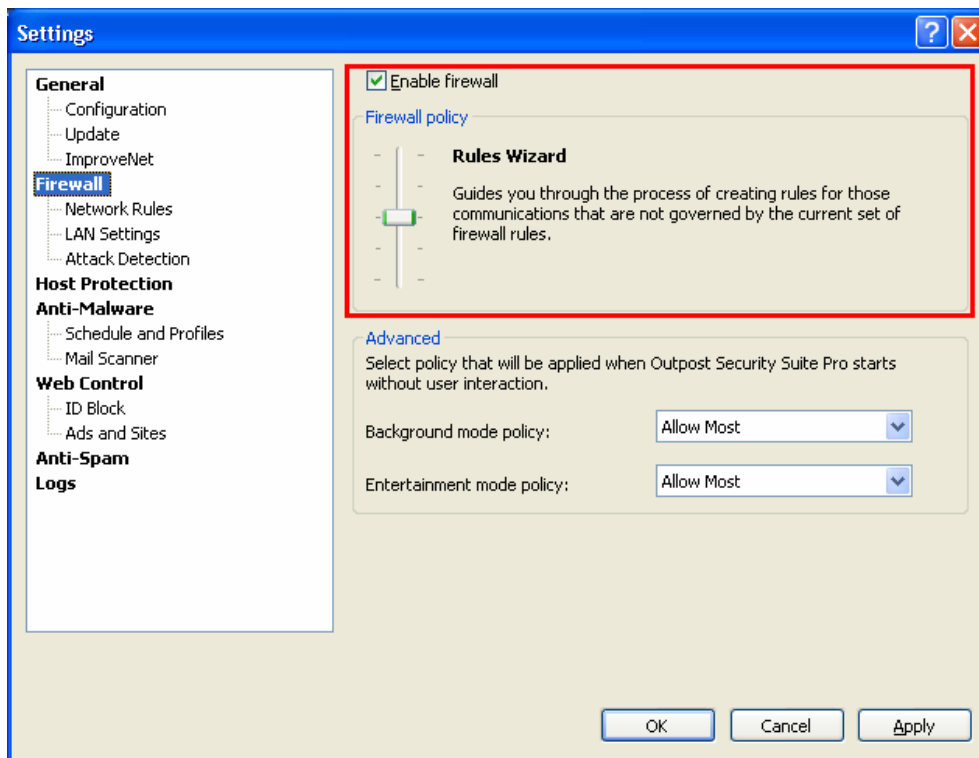


5 Managing network connections

As the use of the Internet continues to grow, so does the need to protect your online privacy and the confidential data stored on your PC. Your connection also needs to be secured, so hackers can't threaten the security of your computer while it is connected to the Internet or a home network.

Outpost Security Suite Pro firewall provides a wide choice of protection levels all the way from totally blocking all Internet access of every application on your computer to allowing full access to every application.





To enable the firewall, click **Settings > Firewall** and select the **Enable firewall** check box:




5.1 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 | All network connections are allowed except those that are explicitly blocked by global |

| | | |
|--|------|--|
| | Most | 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:

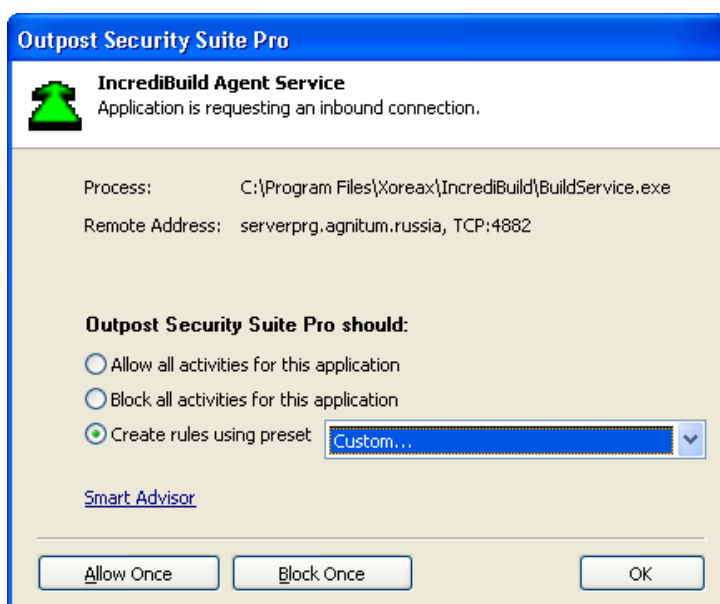
- Because the Rules Wizard policy is not supported when Outpost Security Suite Pro runs in [background](#) or [Entertainment mode](#) (as these modes do not include interaction with the user), you need to explicitly specify what firewall policy is to be applied when Outpost Security Suite Pro switches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

5.1.1 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 and the application will be given the **Trusted application** status.

- **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. The application is given the **Blocked application** status.

- **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.

The application will be included in the **Partially allowed applications** list.

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.
- Outpost Security Suite Pro can perform malware scan for all processes requesting network access and having no rules specified. Scan results will be displayed in the Rules wizard prompt header. See [Real-Time Protection](#) for details.
- 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.

5.1.2 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.

5.1.3 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.

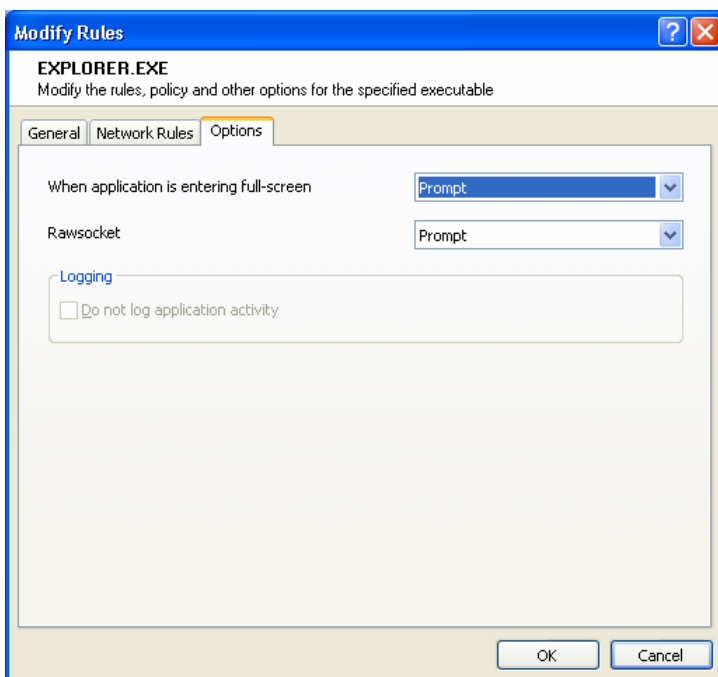
Outpost Security Suite Pro provides a specially designed **Entertainment mode** where protection is active without bothering users with numerous product prompts and alerts. Once the full screen application (a game, media player, etc.) is started, Outpost Security Suite Pro detects this event and suggests 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:



If you want a particular application to always or to never use Entertainment mode without any prompt, select the **Remember for this application** check box before responding to the dialog box. You can also enable or disable Entertainment mode for specific applications by clicking **Settings** on the toolbar, selecting the **Network 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:

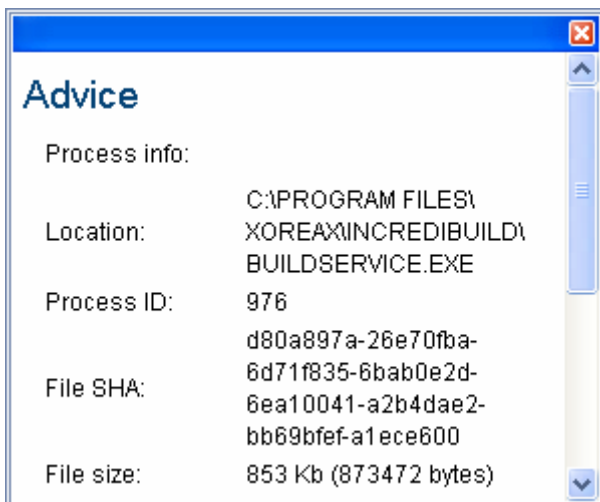
- When operating in background mode, Outpost Security Suite Pro does not need to enter Entertainment mode.
- When an application without network access rules already set enters Entertainment mode, it is put in the **Trusted applications** group.

5.1.4 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.

A Smart Advisor window looks like the following:



5.2 Configuring Local Network Settings

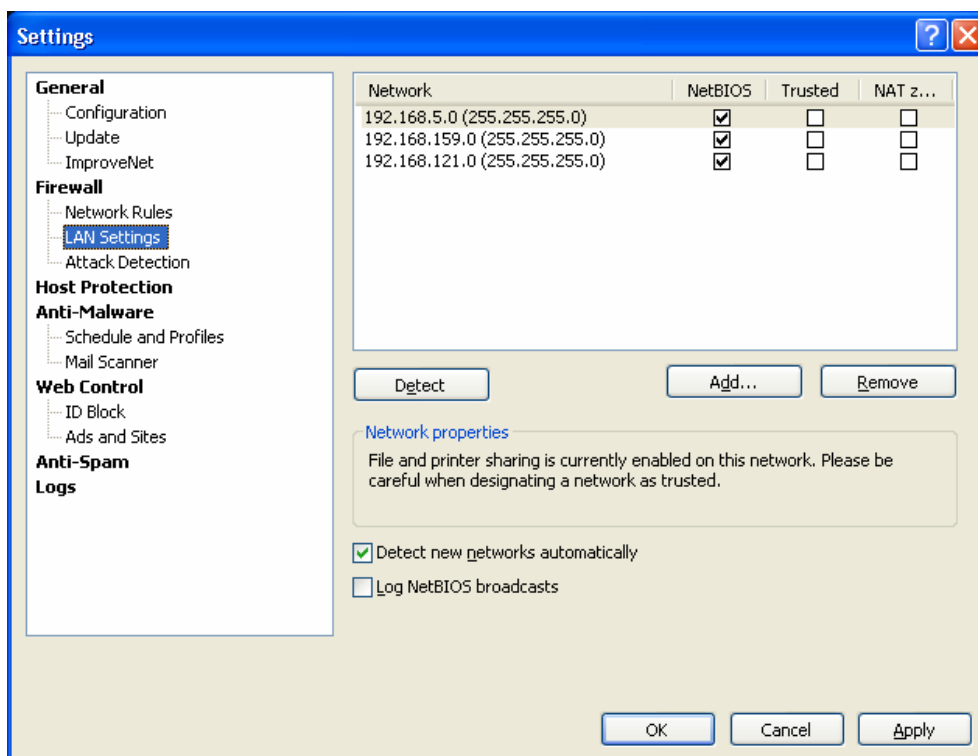
A fundamental difference between a local area network (LAN) and the Internet is the level of trust you can have in each. A LAN used at home or at work is generally comprised of "friendly" computers, computers belonging to or operated by other family members or fellow workers.

Outpost Security Suite Pro lets you [detect the networks](#) your computer belongs to and define the specific [access level](#) for each network.

5.2.1 Detecting a Local Area Network

Normally, LAN settings of your computer are detected and configured during the installation of Outpost Security Suite Pro. You can also detect your LAN any time in order to communicate with other computers.

To view the list of networks to which your computer belongs, click **Settings** on the toolbar and select the **LAN settings** page:



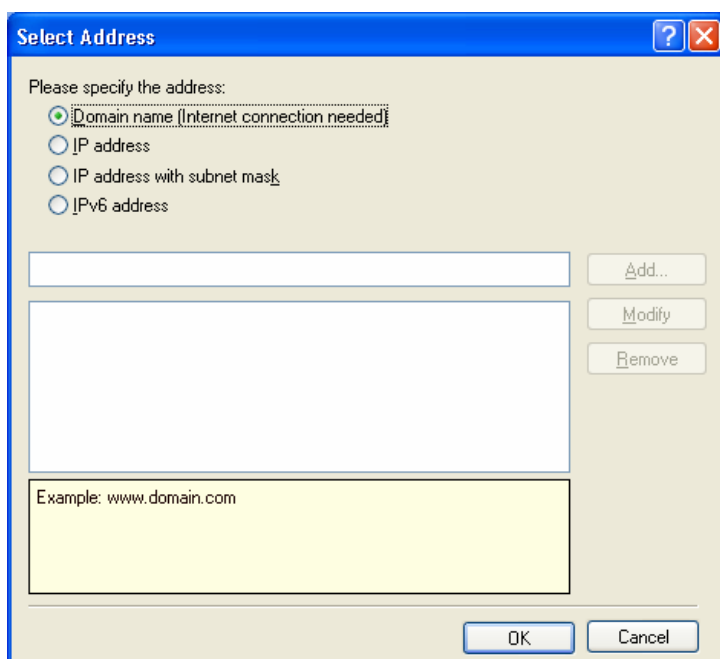
Detecting a LAN automatically

On the **LAN Settings** page, click **Detect** and Outpost Security Suite Pro will automatically discover the networks your computer belongs to and will create a list of their IP addresses, specifying the default level of access for each local detected network. You can then fine-tune the appropriate access levels for each network.

For Outpost Security Suite Pro to automatically detect new networks, so you do not need to add them manually, select the **Detect new networks automatically** check box and click **OK** to save the settings.

Adding a network address manually

If you prefer to manually add a network or remote host to the list and to configure a specific access level for it or if for some reason Outpost Security Suite Pro did not detect your networks automatically, you can do this by going to the **LAN Settings** page, click **Add** and in the **Select Address** dialog specify the format you wish to use to enter the network or host address. The following options are available:



- **Domain name.** For example, www.agnitum.com. An active Internet connection is required for this because the IP address of the domain name needs to be looked up over the Internet. The IP address is saved along with the domain name you enter and it is this IP address that is used by Outpost Security Suite Pro.
- **IP address.** For example, 216.12.219.12.
- **IP address with subnet mask.** For example, 216.12.219.1 - 216.12.219.255.
- **IPv6 address.** For example, 2002::a00:1.

Type in the address in the format you selected (wildcards are allowed) and click **Add**. You can add several addresses in sequence this way and then click **OK** to add them to the list on the **LAN Settings** page. Configure the appropriate access levels for each network and click **OK** to save the settings.

Removing an address from the list

You can remove a selected address or network from the list by clicking the **Remove** button. Removing an address from the list is similar to specifying the **Limited Access to LAN** level for that address (i.e. clearing both the **NetBIOS** and **Trusted** check boxes).

Note:

- For details on configuring LAN access levels, see [Specifying LAN Access Levels](#).

5.2.2 Specifying LAN Access Levels

All computers on a LAN can be assigned one of the following levels of access regarding your computer:

- **NetBIOS** access: only File and Printer Sharing between the LAN and your computer is allowed. To set this level, select the **NetBIOS** check box for this address.
- **Trusted**: all connections to and from the network are allowed. To set this level, select the **Trusted** check box for this address.
- **NAT Zone**: select this check box, if you use Internet Connection Sharing and other computers on the network get Internet access via your computer.
- **Limited Access to LAN**: NetBIOS communications are blocked, all other communications are handled by application and global rules. To set this level, clear both the **NetBIOS** and **Trusted** check boxes for this address.

It is very important to remember that a host on a **Trusted** network is given the highest priority. Even restricted applications can communicate with the host. It is recommended to set *only absolutely trusted* computers as **Trusted**. If you just need File and Printer Sharing, use **NetBIOS** instead of **Trusted**.

If you do not want to clutter up logs with information about NetBIOS broadcast packets, you can disable data logging for all detected hosts and subnets by clearing the **Log NetBIOS broadcasts for detected networks** check box. This will keep the Event Viewer data clearer and may improve computer performance.

Note:

- NetBIOS broadcast packets are inbound or outbound UDP packets with the sender's address belonging to the selected subnet and sent to address 255.255.255.255 from port 137 or 138. Client computers commonly announce their presence on the network using such packets.
- Please note that Outpost Security Suite Pro's protective components are independent from the address access level. For example, even if you add www.agnitum.com to **Trusted** network addresses, its components will still block banners, active content, etc. from this site and perform their common activity regardless of the address access level.

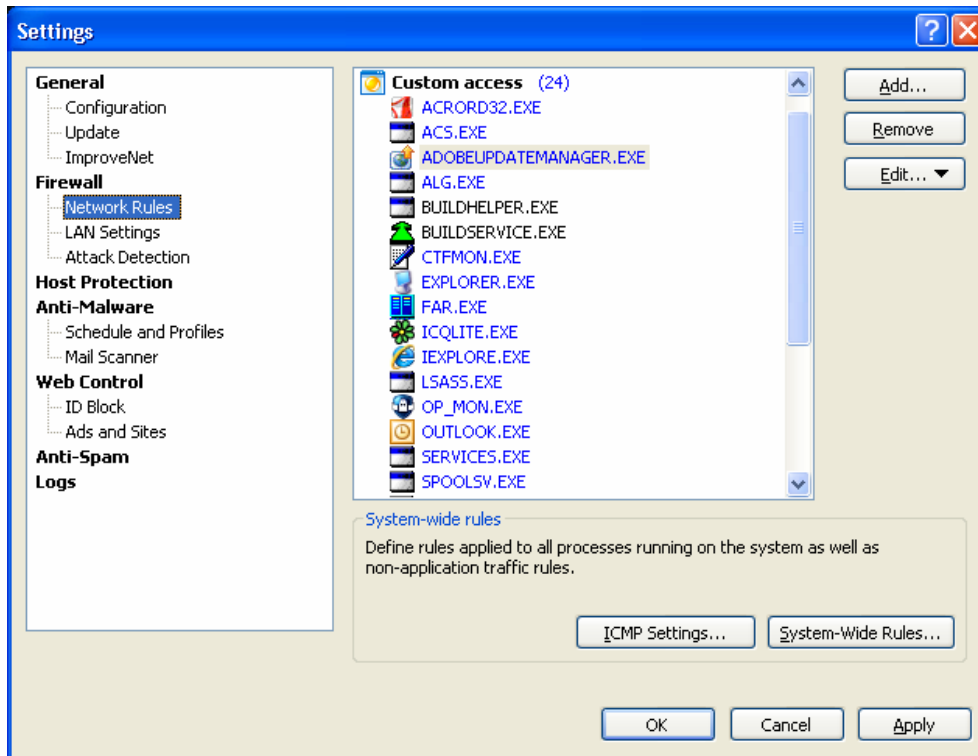
5.3 Managing Applications Network Access

The primary operation of the firewall is granting network access to processes and applications according to specified application rules. This allows for a flexible network access setup and insures that no process can get network access that is not covered by a rule.

Outpost Security Suite Pro generates a list of installed applications and sets the rules for them automatically, but also provides an opportunity to manually manage the [application list](#) and [rules for applications](#). See the appropriate sections for details.

5.3.1 Managing List of Applications

During the initial product [configuration](#), all installed applications are detected and rules for them are created according to built-in presets. To view a list of detected applications, click the **Settings** button on the toolbar and select the **Network Rules** page:



All applications as far as Outpost Security Suite Pro is concerned, are arranged into three groups:

- **Blocked applications**

All network activity of applications in this group is blocked. It is recommended that you add to this group any applications that do not need Internet access, such as text editors, calculators, etc.

- **Partially allowed applications**

Outpost Security Suite Pro allows network access for these applications based on rules that were set by you manually and/or the rule presets. Only closely specified network activity is allowed for these applications. Outpost Security Suite Pro automatically detects installed applications and configures rule presets when you configure the product during installation and it is recommended that you put most applications that were not initially detected by Outpost Security Suite Pro in this group.

- **Trusted applications**

All network activity of applications in this group is allowed. It is not recommended that you include an application in this group unless you absolutely trust it.

You can change the status of an application or process by simply dragging and dropping it into a different group or by right-clicking the application and selecting **Always Trust/Block this Application**.

You can also manage the application list by manually adding applications or removing them. To add an application, select the group in the list and click the **Add** button. You will be prompted to browse to the application's executable and, after adding the file, the **Modify Rules** dialog window will be displayed so you can specify rules for the new application (unless you are adding it to the **Blocked applications** or **Trusted applications** group). After specifying the rules and clicking **OK** you will be able to see the added application in the selected group. For more information on creating and editing application rules, see [Managing Rules for Applications](#). To remove an application from the list, highlight it and click the **Remove** button.

Setting additional application options

The **Modify Rules** dialog also lets you view application executable file details (**General** tab) and set some additional options. Select the **Options** tab to be able to specify the Outpost Security Suite Pro's behavior when an application switches to full-screen mode, as well as rawsocket access control settings.

If you want an application to always or to never use Entertainment mode without a prompt, select the desired action from the **When application is entering full-screen mode** list.

Some applications access a network directly through low-level socket calls, also known as rawsockets. These calls cannot be governed by ordinary protocols and application rules and thus can operate as a backdoor for a rogue application or as a way to access a network without limitations or regulations.

To improve your system's protection, Outpost Security Suite Pro enables you to control rawsocket access. You can define which applications are allowed to make rawsocket calls and which are not by selecting the corresponding option from the **Rawsocket access** list. If you want Outpost Security Suite Pro to ask you each time an application attempts to access rawsockets, select **Prompt**.

Note:

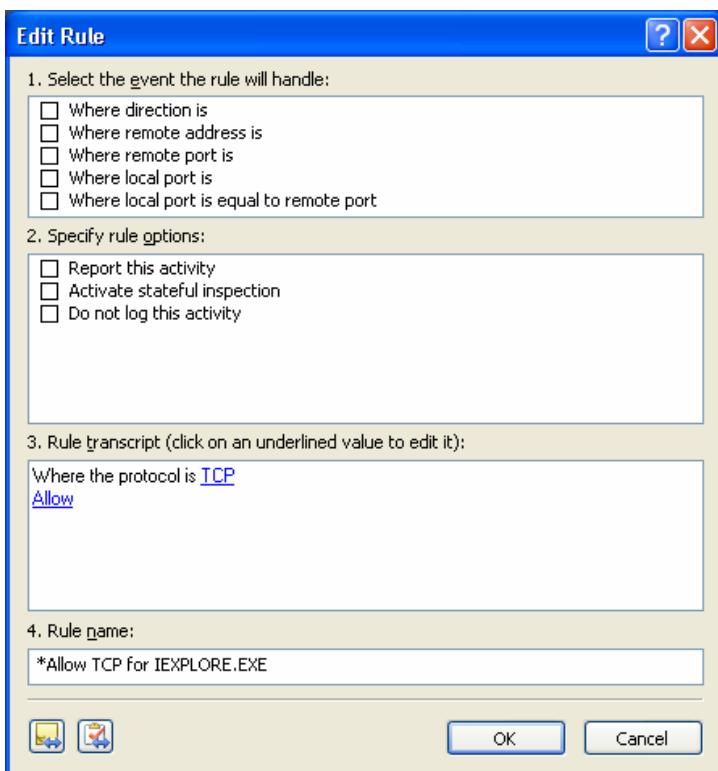
- If you are using the default **Rules Wizard** policy, there is no need to add your applications to the list manually. Outpost Security Suite Pro will suggest rules for each application the first time an app requests network access.

5.3.2 Managing Rules for Applications

To view the existing rules for an application, click **Settings** on the toolbar and select the **Network Rules** page. Double-click the application in the list and select the **Network Rules** tab.

Adding a new rule

To create a new rule, click **New**:



In the rule editor, specify the following rule parameters:

Event the rule will handle

The following criteria are available:

- **Where direction is** – either outbound (data being sent) or inbound (data being removed).
- **Where remote address is** – a specific IP address or DNS name.
- **Where remote port is** – the port on the other computer that will be used.
- **Where local port is** – the port on your computer that will be used.
- **Where local port is equal to remote port** – both computers use the same port number. If port ranges are specified for the remote and local computers, the rule will be triggered for ports that intersect the two ranges. If the intersection is empty, the rule will not be triggered.

Select the criteria of the event and define all the settings in the **Rule description** text box by clicking the underlined links.

Note:

- For information on using macro addresses to specify local or remote host, see [Using Macro Addresses](#).

Rule options

The following actions are available:

- **Report this activity** – the product displays a visual alert when a rule is triggered.
- **Activate stateful inspection** – turns on "stateful inspection" for this application (after an application connects to a remote server, all incoming data from that server – to the port opened by the application – will be allowed or blocked according to the specified setting).

- **Do not log this activity** – disables activity logging for this rule. If selected, no data will be written to the log when this rule is triggered.

Rule description

When you select the event in the above text boxes, corresponding messages will be displayed in the **Rule description** text box. Below the specified commands you will need to state whether to allow or block the connection by clicking one of the underlined links (**Allow** is the default).

Make sure there are no undefined parameters in the **Rule description** text box. Outpost Security Suite Pro will generate a descriptive **Rule name** automatically based on the specified parameters.

Click **OK** to save the rule. The rule will be displayed on the list. The selected rule transcript is shown at the bottom of the window.

Modifying an existing rule

To modify an existing rule, highlight it in the list and click **Modify**. Perform any changes in the rule editor described in the rule creation section above and click **OK** to save the changes.

Selected rules are activated (turned on) and processed by the firewall. Clear the check box next to the rule name to turn it off if you do not want Outpost Security Suite Pro to process the rule but you don't want to delete it either. You can turn the rule on at any time by selecting its check box.

Rules are applied in top-down order (highest on the list is applied first), **so be aware but note that Outpost Security Suite Pro uses the first rule having criteria that match the application's type of communication activity and ignores all subsequent rules**. To change a rule's priority, highlight the rule on the list and use the **Move Up/Down** buttons.

You can also copy or remove the highlighted rule within an application using the **Copy** or **Remove** buttons. To copy a rule from one application to another, use the copy and paste buttons in the **Edit Rule** window.

Tips:

- Use the rule transcript at the bottom of the dialog to quickly change one of its parameters.
- Rules automatically created by Outpost Security Suite Pro are marked **blue** in the list. Rules created by the user are marked **black**.
- It is prudent to save the present configuration before making changes to it.
- For additional information about the rules processing order, see this article: <http://www.agnitum.com/support/kb/article.php?id=1000120&lang=en>.

5.4 Managing Global System Network Activity

Besides controlling network access on [the application level](#), Outpost Security Suite Pro's firewall enables advanced users to control all system traffic on other levels as well.

With Outpost Security Suite Pro, you can:

- Define rules for all processes running on your system ([global rules](#)).
- Define non-application traffic rules ([low-level system rules](#)).
- Control your system's [ICMP traffic](#).

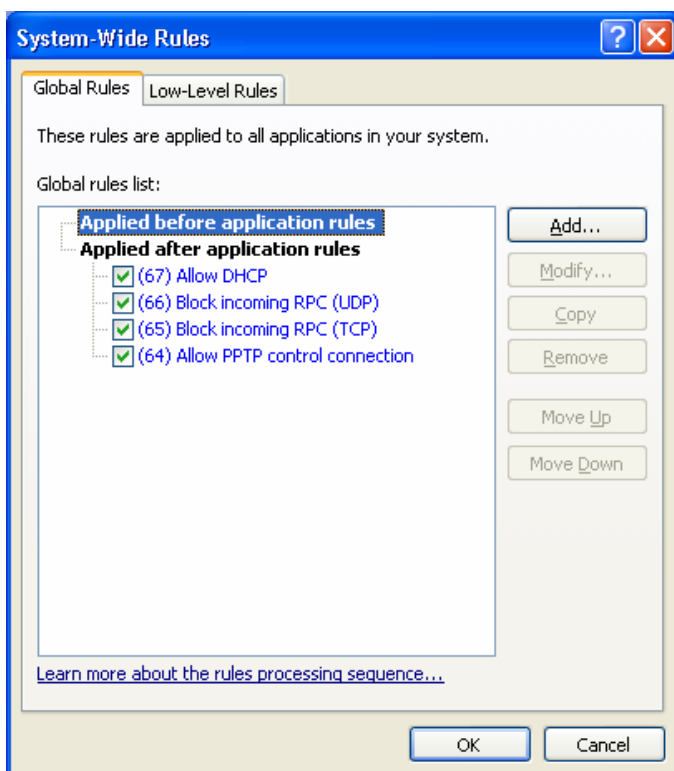
See each corresponding section for details.

Note:

- These settings are for advanced users only. If a setting is changed incorrectly, it could result in your firewall not protecting your system as expected. In most cases, you do not need to modify these rules or add yours.

5.4.1 Managing Global Rules

Global firewall rules are applied to all processes and applications on your computer that request network access. You can, for example, block all traffic that uses the TCP or UDP protocol or all traffic from a particular remote host by creating the appropriate rules. Outpost Security Suite Pro provides several predefined global rules designed for optimal system functioning. To view the global rules list, click **Settings > Network Rules > System-Wide Rules**:



You can add, modify and remove global rules the same way as with [application rules](#).

Selected rules are active (turned on) and processed by the firewall. Clear the check box next to a rule name to turn it off if you do not want Outpost Security Suite Pro to process the rule but you don't want to delete it. You can turn the rule on any time later by selecting its check box.

Rules are applied in top-down order (highest on the list first), **so be aware that Outpost Security Suite Pro uses the first rule that has criteria matching the type of communication activity and ignores all subsequent rules**. To change a rule's priority, highlight the rule on the list and use the **Move Up/Down** buttons. Note that you can set global rules to be processed by the firewall either before or after application rules are applied by placing them appropriately on the list.

You can also copy a highlighted rule or remove a rule by using the **Copy** or **Remove** buttons. It is not recommended to remove any built-in global rules.

Tip:

- Rules automatically created by Outpost Security Suite Pro are marked **blue** in the list. Rules created by a user are marked **black**.

- It is prudent to save the present configuration before making changes to it.
- For additional information about the rules processing sequence, see this article: <http://www.agnitum.com/support/kb/article.php?id=1000120&lang=en>.

5.4.2 Managing Low-Level System Rules

Outpost Security Suite Pro also allows you to control system traffic transferred by protocol drivers that use IP protocols other than TCP or UDP, transit packets, and other non-application traffic that cannot be controlled at the application level.

To view the low-level rules list, click **Settings > Network Rules > System-Wide Rules** and select the **Low-Level Rules** tab.

You can add, modify and remove low-level rules the same way as with [application rules](#). The only differences are:

- Rule criteria contain IP protocol type, direction, remote and local addresses.
- **Mark rule as High Priority** sets a rule higher than application and global rules, which take precedence by default.

Selected rules are active (turned on) and processed by the firewall. Clear the check box next to the rule name to turn it off if you do not want Outpost Security Suite Pro to process the rule but you don't want to delete it. You can turn the rule on any time later by selecting its check box.

Rules are applied in top-down order (highest on the list first), **so note that Outpost Security Suite Pro uses the first rule that has criteria matching the type of communication activity and ignores all subsequent rules**. To change a rule's priority, highlight the rule on the list and use the **Move Up/Down** buttons.

You can also copy a highlighted rule or remove a rule by using the **Copy** or **Remove** buttons. It is not recommended to remove any built-in low-level rules.

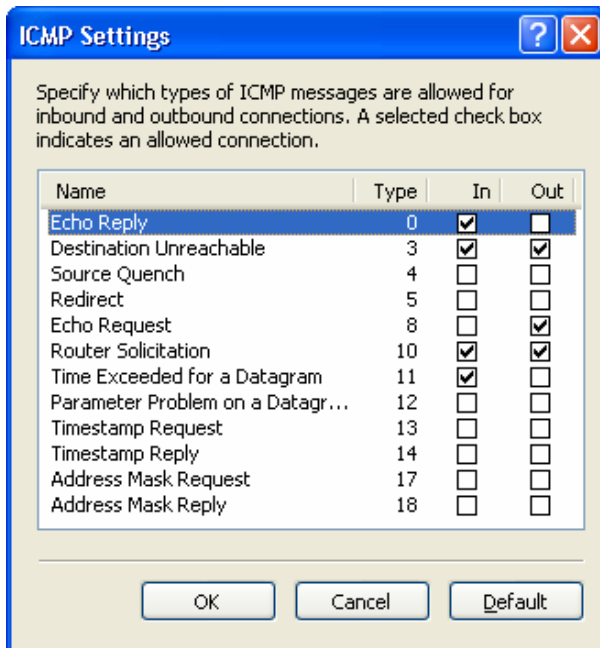
Tip:

- Rules automatically created by Outpost Security Suite Pro are marked **blue** in the list. Rules created by a user are marked **black**.
- It is prudent to save the present configuration before making changes to it.
- For additional information about the rules processing sequence, see this article: <http://www.agnitum.com/support/kb/article.php?id=1000120&lang=en>.

5.4.3 Controlling ICMP Protocol Activity

Internet Control Message Protocol (ICMP) is used to send error/control messages between computers connected on a network. Outpost Security Suite Pro lets you specify the types and directions of the ICMP messages allowed.

To specify the ICMP settings, click **Settings > Network Rules** under **Firewall** and click **ICMP Settings**. In the **ICMP Settings** dialog, the main ICMP message types are listed. You can allow incoming or outgoing messages by selecting the corresponding check boxes by their side. If a check box is cleared, the connection is blocked:



Use the **Default** button to reset all the ICMP settings to the default ones.

Note:

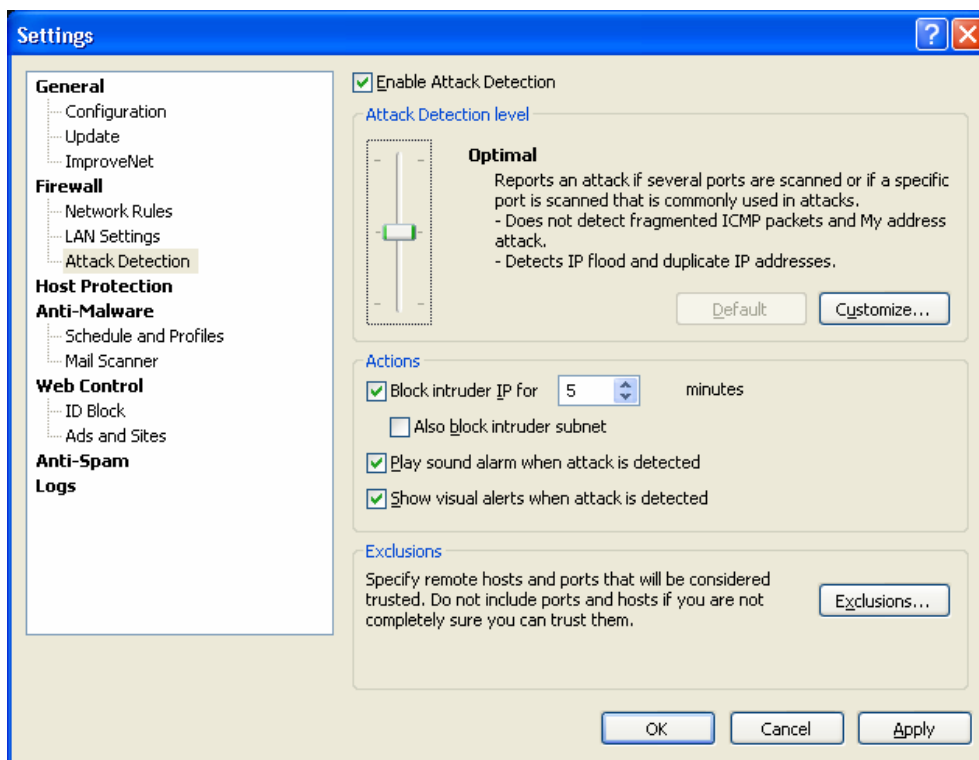
- It is recommended that you do not change the ICMP settings unless you are certain about the changes you are making.

6 Preventing Network Attacks

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

The Attack Detection component detects, prevents, and reports all possible attacks on your computer from the Internet or the network your computer is connected to. It screens inbound traffic and determines its legitimacy either by comparing it against a set of known attack patterns or by performing a behavior evaluation analysis. The Attack Detection component can detect not only every known type of attack (such as port scanning, Denial of Service (DoS), attacks of 'short fragments' and 'my address' classes, and many others), but future exploits as well.

To enable the Attack Detection component, click **Settings > Attack Detection** and select the **Enable Attack Detection** check box:



6.1 Specifying Attack Detection Level

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

- **Maximum.** A port scan alert is displayed even when a single scan of one of your ports is detected. All Ethernet and external attacks are monitored for and prevented.
- **Optimal.** A port scan alert is displayed only when several ports are scanned or if a specific port is scanned that Outpost Security Suite Pro recognizes as one commonly used in attacks. All external attacks are monitored for except fragmented ICMP and My address attacks. IP spoofing and duplicate IP's are watched for.
- **Low.** A port scan alert is displayed only when a multiple scanning is definitely detected. Fragmented ICMP, My address and all Ethernet attacks are not monitored.

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

You may also customize the security level to better meet your requirements by clicking the **Customize** button. The **Ethernet** tab lets you specify settings for [Ethernet attacks](#), the **Advanced** tab will help you define a [list of attacks](#) detected by the firewall and especially protected [vulnerable ports](#).

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

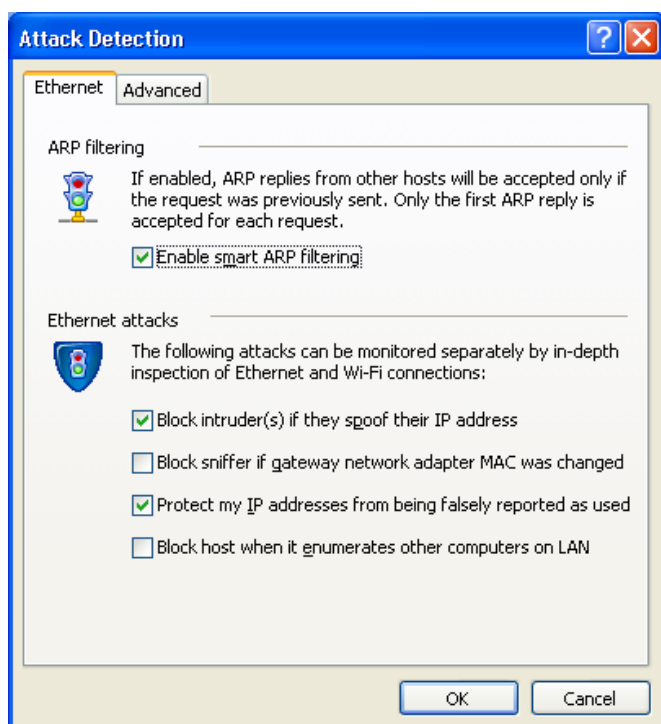
You can also set to block the entire subnet the attacker's address belongs to by selecting **Also block intruder subnet**.

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

6.2 Protecting from Ethernet Attacks

When data is sent from one computer to another over a local network, the sending machine broadcasts an ARP (IP-to-Ethernet address lookup) request to determine the MAC address based on the IP address of the target machine and waits for it to send back its MAC address. During the time between the packet broadcast and the MAC address response, data is vulnerable to tampering, hijacking, and/or redirection to an unauthorized third party.

The Attack Detection component also protects your system from invasions on a local network. It detects and blocks Ethernet attacks such as IP spoofing, ARP scanning, ARP flood and others by inspecting your Ethernet and/or Wi-Fi connections. To specify the Ethernet attack prevention settings, click **Settings > Attack Detection > Customize:**



The following options are available:

- **Enable smart ARP filtering**

Prevents ARP spoofing – where a node starts sending a huge number of ARP replies with varying MAC addresses in a short time span, trying to overload the network equipment as it tries to determine which MAC address actually belongs to the node. If enabled, Outpost Security Suite Pro only permits incoming replies from other hosts for which there was a previous outgoing request. Only the first ARP reply is accepted for each request. Smart ARP filtering also protects from ARP cache poisoning, which occurs when someone succeeds in intercepting Ethernet traffic using fake ARP replies in an effort to change the address of a network card to one that an attacker can monitor. Additionally, it prevents ARP floods where a huge number of bogus ARP replies are sent to the target machine freezing a system.

- **Block intruder(s) if they spoof their IP address**

Detects when an attacker falsifies or forges his IP address and blocks abnormal volumes of traffic, which may otherwise overload a computer. This option cannot stop the network from being flooded, but can protect the PC from overload.

- **Block sniffer if the gateway network adapter MAC was changed**

Outpost Security Suite Pro detects any attempt by an attacker to associate a gateway network adapter IP address with their own MAC address to allow them to intercept packets. Hackers can substitute legitimate MAC addresses with ones of their own and reroute legitimate traffic to a hacker-controlled machine, by sending out forged ARP responses, which Outpost Security Suite Pro will detect and block. This ARP spoofing enables hackers to be able to 'sniff' (read) packets and view any data in transit, to direct traffic to non-existent hardware causing delays in data transmission or a denial of service on the affected equipment. Specialized hacker sniffing programs can also intercept traffic, including chat sessions and related private data such as password entries, names, addresses, and even encrypted files, by modifying MAC addresses at the Internet gateway.

- **Protect my IP addresses from being falsely reported as used**

Outpost Security Suite Pro detects cases where two or more hosts share the same IP address. This can be due to an attacker attempting to gain access to network traffic or block a computer from accessing the network, but could also happen legitimately where an ISP uses multiple servers for load-sharing. If enabled, Outpost Security Suite Pro blocks ARP replies that have the same IP (but different MAC's) and thus protects the computer from IP address duplication consequences.

- **Block hosts enumerating other computers on LAN**

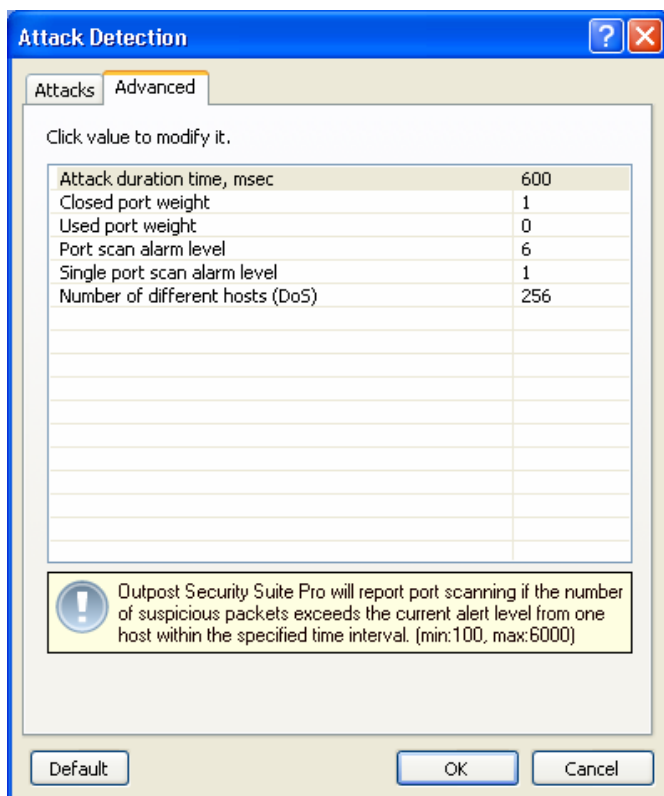
Limits the number of ARP requests enumerating IP addresses from one MAC address during a specified time interval, which can imply network scanning. Some massively propagating viruses use mass host enumeration to hop from one computer to another, infecting them as they go. This technique is also used by scanners and vulnerability analyzers.

6.3 Port Scanning

Outpost Security Suite Pro's Attack Detection component performs two independent functions, it blocks attacks and detects port scanning. In this context, an attack is the sending of harmful data to your computer, which can result in system errors (BSOD, system freeze, etc.) or an attempt by an attacker to gain unauthorized access to the data on your computer. Port scanning is an attempt to discover open ports in your system prior to an attack.

On receiving a connection request (a brief message in computer lingo that seeks to establish a connection through one of the ports on your computer), the Attack Detection component logs "Connection request", but to avoid false positives, does not consider this one request a port scan. If multiple connection requests are received from the same remote host, the plug-in will alert you with "Port scanning".

Outpost Security Suite Pro's sensitivity in detecting port scanning (which is actually the number of connection requests that trigger a "Port scanning" alert) is defined by the **Port scan alarm level** setting (**Settings > Attack Detection > Customize > Advanced > Edit List > Advanced**):



By default, the number of port requests from the same host that triggers an alert for each attack [detection level](#) is: 2 for **Maximum**, 6 for **Optimal**, and 12 for **Low**.

Paying special attention to vulnerable ports

From the security point of view TCP and UDP ports in your system are divided into several groups according to the probability of an attacker using the port to break into your system. Typically, ports assigned to vulnerable services like DCOM or RPC should be monitored with greater care because they are more likely to be an attack target.

However, you may have custom services assigned to custom ports that are also a lure for an attacker. The Attack Detection component lets you set selective preferences for different ports and create a list of ports to which Outpost Security Suite Pro will pay more attention while monitoring network traffic.

On receiving a connection request to a port that can be used by a vulnerable service, (for examples, 80, 21, 23, 445, etc.), the plug-in will not consider it a single request, but as a number (X) of connection requests performed by the remote host, where X is the weight (importance) assigned to that port. A port's weight is a decimal value that indicates that port's vulnerability or likelihood of being used in an attack. A greater number indicates a more vulnerable port.

The weights of all ports to which requests were sent during a specified time interval are summarized and if this number exceeds the current port scan alarm level, a "Port scanning" alert will be displayed.

There is no way to determine with certainty if your computer is being port scanned (someone trying to see if there's a vulnerable port open). It is very much like having a stranger covertly glance at you several times. The question is how many glances (or ports scanned) before you start to become concerned. By setting the Attack Detection sensitivity you define the maximum number of attempts to connect to your computer before the "Port scanning" alarm is triggered.

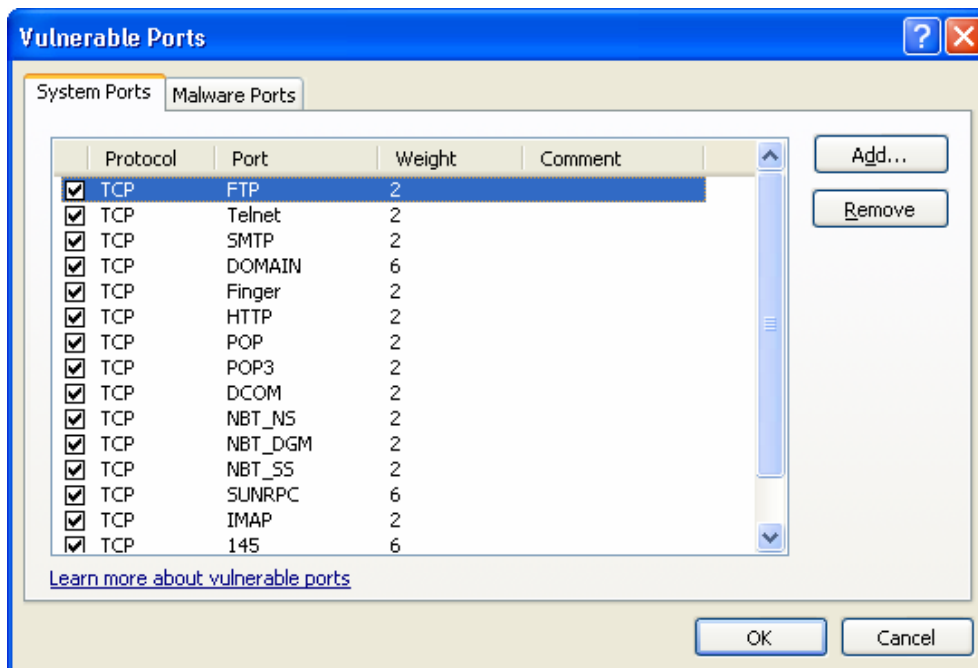
Example

Let the Attack Detection level be set to **Optimal**;
 Vulnerable port 80 weight is set to 7;
 Vulnerable port 21 weight is set to 3.

A "Port scanning" alert will be displayed if a remote host:

- Attempts to connect to your system's port 80 one time.
- Attempts to connect to your port 21 once and to any other port three times.
- Attempts to connect to any other ports on your computer six times.

To specify a port that you consider vulnerable and to view the port weights, click **Settings > Attack Detection > Customize > Advanced** and click **Specify** under **Vulnerable ports**. Unlisted ports have weights specified by the **Closed port weight** and **Open port weight** settings:



Vulnerable ports are divided in two groups: **system ports** and **malware ports**. Add ports that are used by vulnerable system services to the system ports list. Add ports that are exploited by well-known malware to the malware ports list. Select the tab according to the list you want to change.

To add a port, click **Add** and specify the following parameters: protocol, port number and weight. Weight is a decimal value that indicates that port's importance. A greater number indicates a more vulnerable port. You may also add optional comments in the corresponding field to describe the port's purpose or anything else you'd like noted.

Click **OK** to add the port to the list.

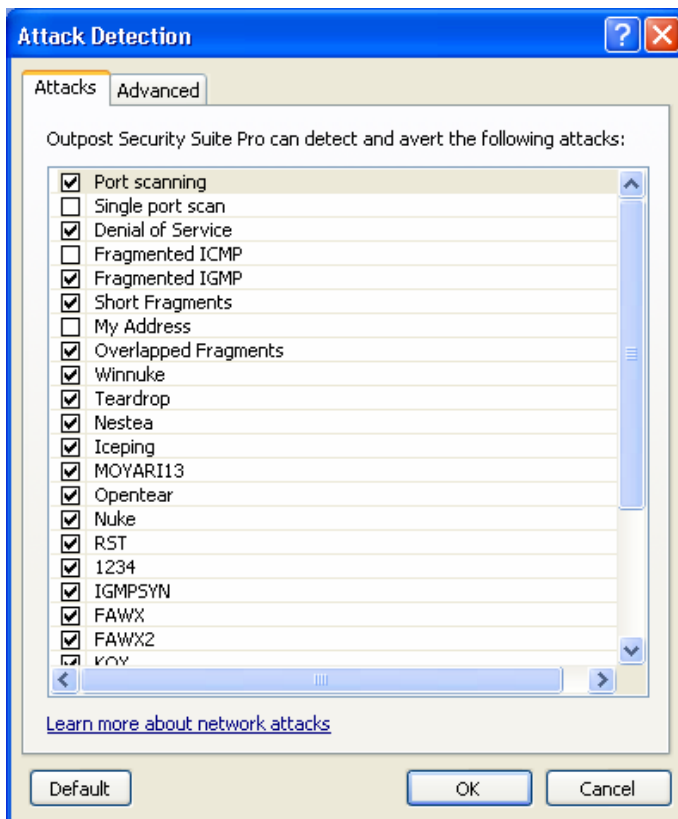
Note:

- To specify the time interval for detecting port scanning, edit the **Attack duration time** setting (**Settings > Attack Detection > Customize > Advanced > Edit List > Advanced**).
- For additional information about ports that might be abused, see this article: <http://www.agnitum.com/support/kb/article.php?id=1000242&lang=en>.

6.4 Attacks List

You can designate the attacks Outpost Security Suite Pro is to detect and block. By default, more than 25 different types of attacks or exploits are handled, but you can select not to detect certain types to lower your system resource usage or to stop too-frequent or faulty alert messages that may appear if, for example, a trusted service in your network is falsely perceived as an attack source.

To customize the attack detection list, click **Edit list** on the **Advanced** tab, having clicked **Settings > Attack Detection > Customize**:



All the selected types of attacks are detected by the firewall. To exclude a type, clear its check box. To revert to the default settings, click **Default**.

Note:

- For additional information about attack types, see this article: <http://www.agnitum.com/support/kb/article.php?id=1000193&lang=en>.

6.5 Specifying Trusted Hosts and Ports

There may be computers that you are absolutely sure are not a source of danger to your system as well as ports on your system you are sure cannot serve as an intruder's backdoor. In other words, you consider any monitoring of these hosts and ports unnecessary and prefer to conserve system resources and performance by not monitoring them. The Attack Detection component features exclusion lists to which you can add hosts and ports you don't want to be monitored.

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

Specifying trusted hosts

On the **Hosts and Subnets** tab, click **Add** and in the **Select Address** dialog specify the format you wish to use to enter the network or host address. The following options are available:

- **Domain name.** For example, www.agnitum.com. An active Internet connection is required for this because the IP address needs to be looked up over the Internet. The IP address is saved along with the domain name you enter and it is this IP address that is used by Outpost Security Suite Pro.

- **IP address.** For example, 216.12.219.12.
- **IP address with subnet mask.** For example, 216.12.219.1 - 216.12.219.255.
- **IPv6 address.** For example, 2002::a00:1.
- **Macro address.** For example, LOCAL_NETWORK. For information on using macro addresses to specify local or remote host, see [Using Macro Addresses](#).

Type in the desired address in the format you selected (wildcards are allowed) and click **Add**. You can add several addresses in sequence this way and then click **OK** to add them to the trusted list. To remove an address from the list, select it and click **Remove**.

To disable detection of attacks from gateways, clear the **Check traffic from gateway hosts** check box. Specify all hosts and subnets you consider trusted and click **OK** to save the settings.

Specifying trusted ports

Select the **TCP Ports** or **UDP Ports** tab depending on the port(s) you are going to add to the trusted list. You can either enter the port number or port range, separated by commas, in the text box provided or select the required port from the list and double-click it to add it to the text box.

To remove a port from the list, simply erase its name or number in the text box.

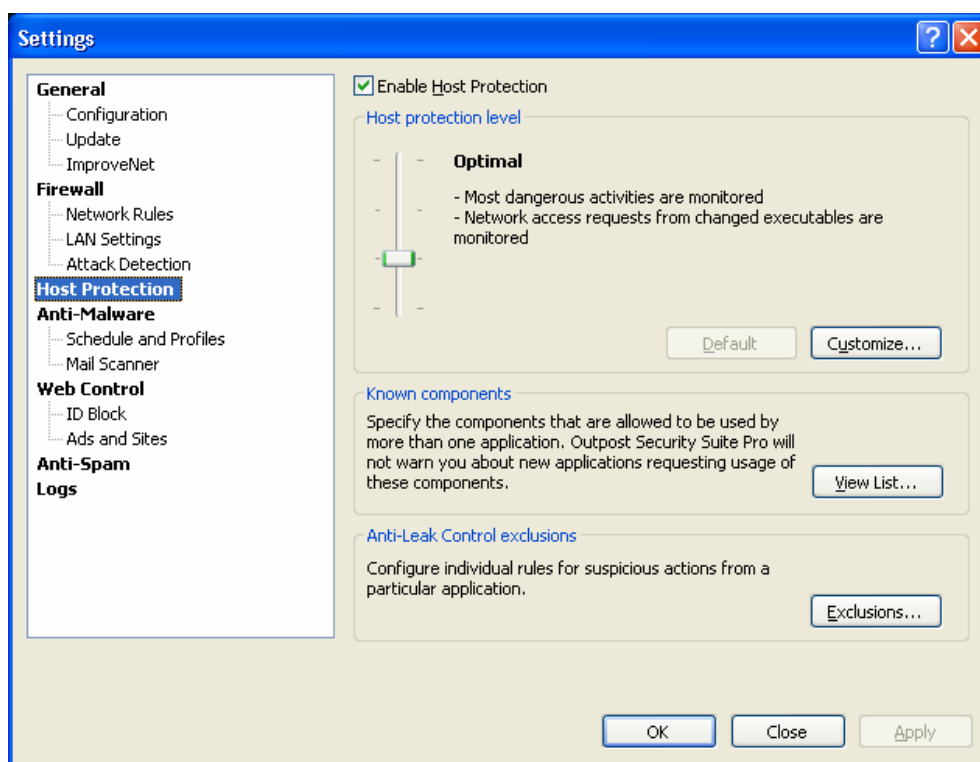
After specifying all the ports, click **OK** to save the settings.

7 Protecting a Host from Malicious Process Activity

Some malicious applications can be activated as parts of legitimate programs and perform their activity on behalf of a trusted application. For example, some Trojan horses can be injected into a computer system as a module of a legitimate application (such as your browser) and thus gain the privileges needed to connect to the person who configured the Trojan. Others can start processes in hidden mode or hijack trusted process memory to pretend to be an application you do not consider harmful.

Outpost Security Suite Pro's Host Protection does not allow such program activity and thus fully protects you from Trojans, spyware and other dangers. By employing technologies of [Component Control](#), [Anti-Leak Control](#), and [Critical System Objects Control](#) it provides the first line of defense against rogue software by proactively controlling how programs behave and interact on a PC.

To enable Host Protection, click **Settings** on the toolbar, select the **Host Protection** page, and select the **Enable Host Protection** check box:



It is not recommended to disable Host Protection. You might disable it when you experience significantly reduced performance, crashes, or other errors that lead to system instability and you want to verify that these instabilities are not being caused by Outpost Security Suite Pro. Turning Host Protection off severely reduces your system's security level, as it is no longer having each system activity monitored.

7.1 Setting Local Security Level

The current degree of protection is characterized by the local security level setting which represents the combination of specific [Anti-Leak Control](#), [Component Control](#), and [Critical System Objects Control](#) settings providing the level of host security.

The initial security level is specified during installation while creating the product configuration and can be modified at any time later according to your needs.

To change the security level, click **Settings** on the toolbar and select the **Host Protection** page. The following security levels are available:

- **Maximum.** Provides the best protection against all penetration techniques that are often used by malicious software to bypass security software. Network requests from all new or changed

application components are monitored. The launching of all new or changed executables is monitored. Changes of all critical objects are monitored. Having selected this level, you will get a lot of product prompts that require your response, therefore it is recommended for advanced users.

- **Advanced.** Ensures protection against all penetration techniques that are often used by malicious software to bypass security software. Network requests from changed executables are monitored. The launching of changed executables is monitored. Changes of all critical objects are monitored.
- **Optimal.** Provides protection against the most dangerous penetration techniques. Network requests only from changed executables are monitored. Changes of all critical objects are monitored. If selected, some of the more exotic security test programs (leaktests) will fail.
- **Low.** If you select this option, Anti-Leak Control and Critical System Object Control are disabled completely. Only changed executables are monitored. This produces the minimal number of product prompts.

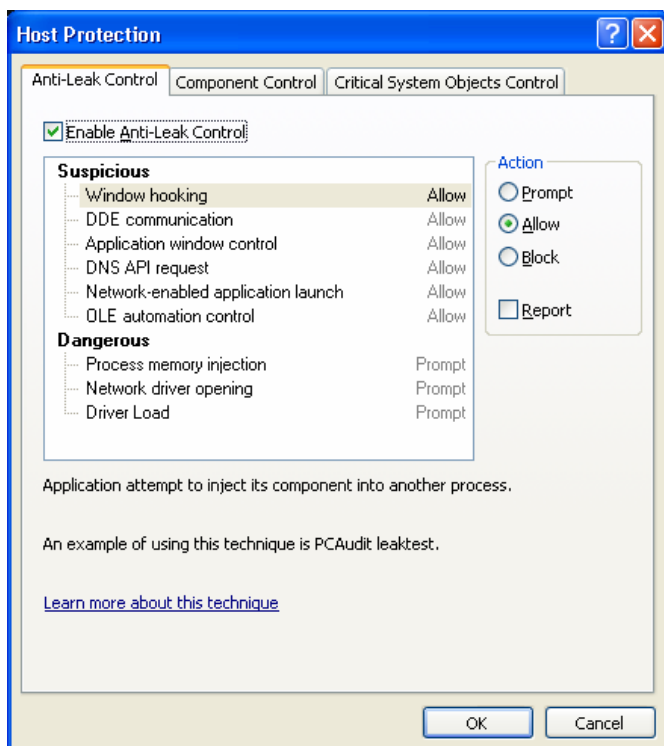
To customize your security level to better suit your needs, click **Customize**. In the appeared dialog box you can set parameters for [Anti-Leak Control](#), [Component Control](#) and [Critical System Objects Control](#) according to your specific requirements.

To restore the default security level, click **Default**.

7.2 Controlling Penetration Techniques

There are several advanced penetration schemes that allow malicious software to bypass the security perimeter of a PC. Outpost Security Suite Pro provides proactive security functionality called **Anti-Leak Control** that blocks all currently-known penetration techniques that are often used by malicious programs to bypass security software (for details, see [Understanding Penetration Techniques](#)). This prevents sensitive data leakage from individual PCs, gives more control over what's happening on a PC, and alerts you to spyware programs that use sophisticated techniques to hide themselves. However, some of these techniques can be used by legitimate applications in their regular activity, so it is necessary to be able to flexibly control them as simply blocking the activity can affect system stability and interrupt the user's work.

To enable Anti-Leak Control, click **Settings** on the toolbar, select **Host Protection**, click the **Customize** button, and select the **Enable Anti-Leak Control** check box. The available settings allow you to select the actions all applications in your system are allowed to perform. All actions are divided into *dangerous*, which are critical and most likely will result in system instability and data leaks; and *suspicious*, which sometimes can be used by legitimate applications for their routine activity:



Select an action on the list and the right part of the window will show you its settings and below that the element's description is displayed. The default setting for each action depends on the security level you chose during installation. To allow or block a particular action globally for the system, select one of these available options:

- **Prompt.** Outpost Security Suite Pro will prompt you each time an application tries to perform the selected activity.
- **Allow.** The selected activity will always be allowed for all applications on your system.
- **Block.** The selected activity will always be blocked for all applications on your system.

Besides these options, you can also have Outpost Security Suite Pro show a visual notification each time an action is allowed or blocked for the application by selecting the **Report** check box.

To individually set rules for suspicious actions from a particular application (for example, to allow a specific application to modify the memory of other processes), click the **Exclusions** button under **Anti-Leak exclusions** on the **Host Protection** page. Click **Add** and browse to the application's executable file. After clicking **Open**, you will see the application on the list and will be able to specify its individual anti-leak settings. To change the settings for the selected action, click the link in the **Action** column next to the action name. The available actions are the same as for the global system settings described above. You can also set to inherit global setting for the action, specifying the **Use Global** setting.

Click **OK** to save your settings.

Note:

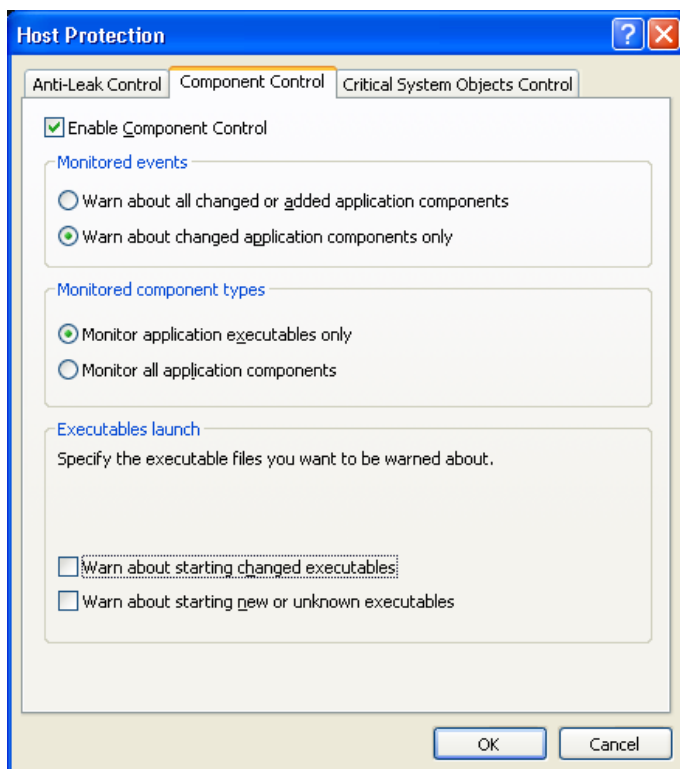
- Any actions that are performed over other instances of the same process are allowed. For example, Internet Explorer can control other Internet Explorer windows.

7.3 Controlling Application Components

Applications typically have dozens of modules, any of which can easily be substituted by a virus or Trojan made to execute a malicious code on your computer. Outpost Security Suite Pro does not just monitor applications but also each component of each application. If a component of an application has been

changed and the application is about to establish a connection, Outpost Security Suite Pro will inform you of the changed component and ask whether this connection should be allowed. The technology used is called **Component Control** and its purpose is to make sure no fake or malicious components get network access.

To change the Component Control settings, click **Settings > Host Protection > Customize** and select the **Component Control** tab. To enable/disable Component Control, select/clear the **Enable Component Control** check box:



To specify whether Outpost Security Suite Pro should monitor all components that are being registered as part of a legitimate application or only components that are changed, use the options under **Monitored events**.

To decide, whether to warn about every changed or added application component or only about executable files, use the options under **Monitored component types**.

Under **Executable launch**, you can set Outpost Security Suite Pro to control the launch of changed and/or new executable files.

Each time a monitored event occurs, Outpost Security Suite Pro displays a learning dialog box that prompts for future action, to either allow the application activity (and update information about new or changed components) or block the file running.

The Component Control prompt looks like the following:



If you do not know about the executable, you can click the **Details** button to see more information about it.

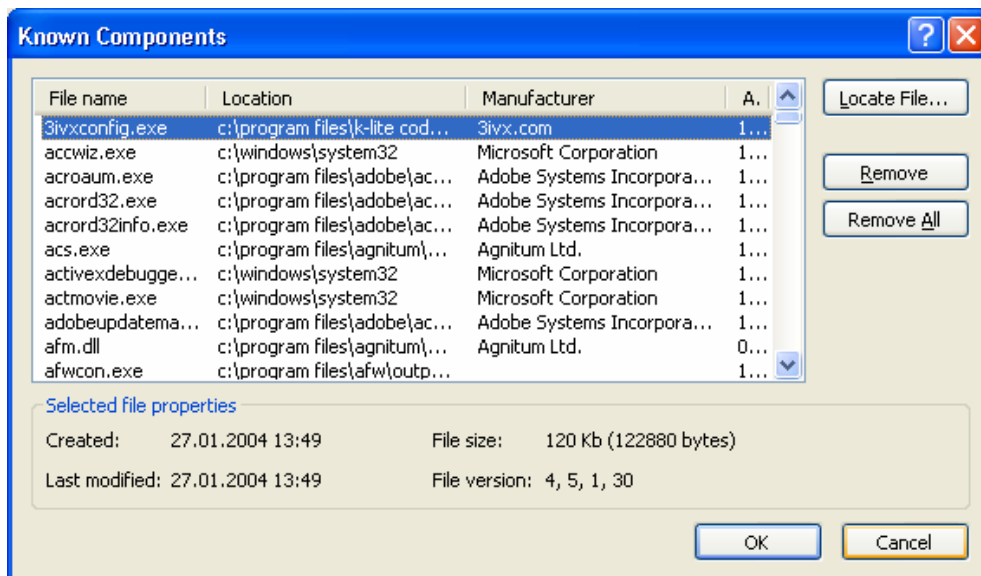
Tip:

- Known components are marked **red** and components of a specific application are marked **green**.
- To improve check performance, you can have Outpost Security Suite Pro create check status cache files in each folder by selecting the **Enable SmartScan technology** check box on the **General** page of the product properties. Note, that the cache files are invisible and therefore may cause false positives from anti-rootkit tools.

Managing known components

You can manage the components that are allowed to be used by applications installed on your computer. Outpost Security Suite Pro will not warn you when a component from this list is requested by an application to which it is not registered. By default, all Windows system components are added to this list because they are used by most Windows applications. You can, however, modify the list to match your specific needs.

To modify the components list, click **View List** under **Known components** on the **Host Protection** page:



Components are added to this list automatically after user responses to update information about a changed component in a Component Control prompt. If you want information about the component to be updated next time some application attempts to use it, remove the component from this list using the corresponding button.

To open the folder where the highlighted component is stored, click the **Locate File** button.

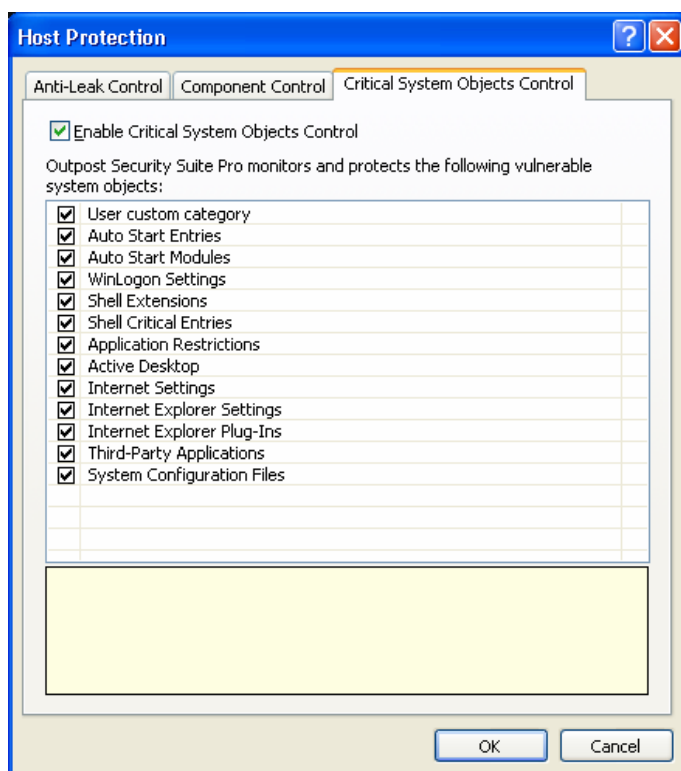
7.4 Controlling Critical System Objects

When you install any new software on your system, it registers its components in critical areas of the system registry. This is so the system does not interfere with a new program's performance.

Malware tends to register within critical system objects as well so it can freely perform its activities and arouse no suspicion within security products. Therefore, before starting its main activities of breaking system stability or security, malware tries to modify critical entries for its needs.

To prevent this, Outpost Security Suite Pro protects the most critically important system objects. It warns a user if any executable file tries to modify them and prompts for further action.

A list of critical system objects that are protected from malicious and accidental changes by various applications is available by clicking **Settings > Host Protection > Customize > Critical System Objects Control** tab:



To learn more about each object, highlight it and you will see its description below.

To enable Critical System Objects Control, select the **Enable Critical System Objects Control** check box. If you do not want a particular object to be monitored by Outpost Security Suite Pro, clear its check box. You will always be able to restore the default settings at any time.

8 Protecting against Malware

Malware is a growing problem that affects many personal computer users. In increasing frequency users are unknowingly confronted by malicious programs that infect their systems, collect information about their web surfing habits, send their computers' installed applications and other private data to third parties, and track their actions without their consent. Malware can change e-mail texts, modify files on your hard disk, display annoying ads, and change your browser's homepage. If all those weren't enough reasons to be alarmed, resident malware requires system resources, which slows down your computer, dramatically in some cases.

The Anti-Malware component is designed to prevent unwanted and unauthorized actions being performed by malware. Both antivirus and anti-spyware capabilities are provided through the universal component to ensure that your computer is kept clean of any malicious programs that might infect it while you're surfing the web or otherwise working.

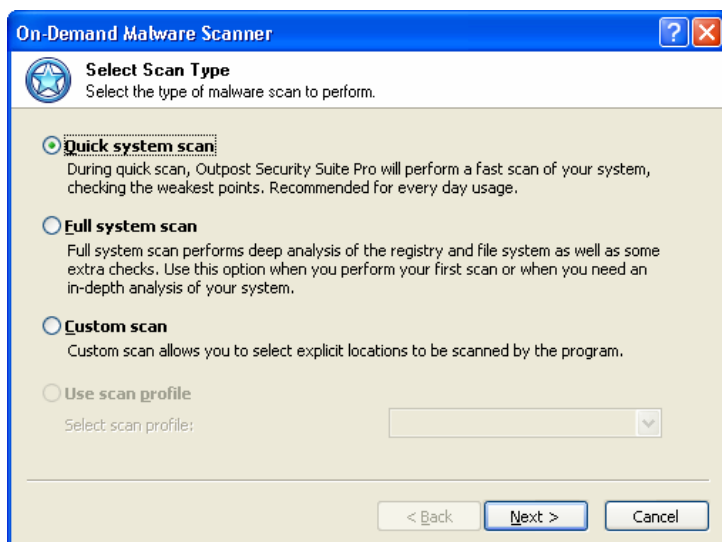
8.1 Performing a System Scan

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](#).

8.1.1 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.

Creating a scan profile

A scan profile is a set of predefined scan settings to be applied and used during a system scan. Having created a scan profile with settings that suit your requirements, you relieve yourself from the need to specify the same settings each time you want to perform a scan. Instead, you simply select the profile name from the list and all the settings stored in that profile are used to scan your system.

To create a new scan profile, click **Settings > Schedule and Profiles** and under **Scan Profiles** click **New**. In the dialog box, give a descriptive name to your new profile and click **OK** to continue.

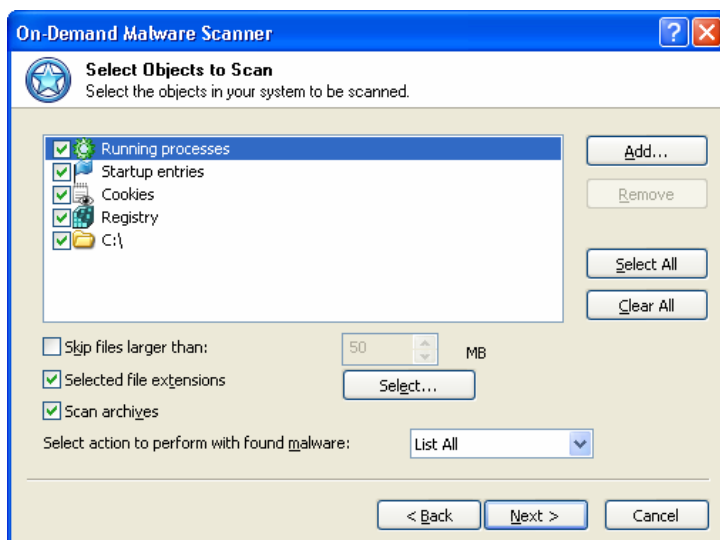
In the **Edit Scan Profile** window, you will be able to specify [the objects to be scanned and other scanning settings](#). After specifying the settings, click **OK** to save your profile and it will be displayed in the **Scan Profiles** list.

Each profile can be edited or removed (except the default **Full Scan** and **Quick Scan** profiles) any time later by clicking the corresponding buttons.

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

8.1.2 Selecting Objects to Scan

If **Custom scan** is selected, the **Select Objects to Scan** step appears for you to explicitly select the objects, disks, folders, and files you want to have scanned and the actions to be performed on any detected malware objects. The same settings are available for editing a scan profile in the **Edit Scan Profile** window:



To add a folder to the list, click the **Add** button and in the **Select Folders** window, browse to and select the particular locations. Click **OK** to add the folders. To remove a selected object, click **Remove**.

If you do not want to scan files larger than a specific size, select the **Skip files larger than** check box and specify the minimum file size to be skipped. You can also limit scans to specified types of files by selecting the **Select file extensions** check box. To edit the list of file extensions to process, click the **Extensions** button. The most common types of files that can contain malicious code are already added to the list for your convenience, but you can add, edit, or remove file extensions according to your needs. To revert to the original list, click the **Default** button.

To configure scanner behavior, specify the action to perform on found malware. The following actions can be performed on suspicious programs:

- **List All.** In this case, all the detected objects will be listed after the scan is finished and you will be able to process each object individually. See [Removing Detected Malware](#) for details.
- **Cure.** On detecting a suspicious program, Outpost Security Suite Pro will try to cure the suspicious object. If the object cannot be cured, Outpost Security Suite Pro will automatically quarantine it.
- **Quarantine.** Outpost Security Suite Pro will place the detected malware in [quarantine](#).

If you think your archive files may contain malicious programs, you can also select the **Scan archives** check box.

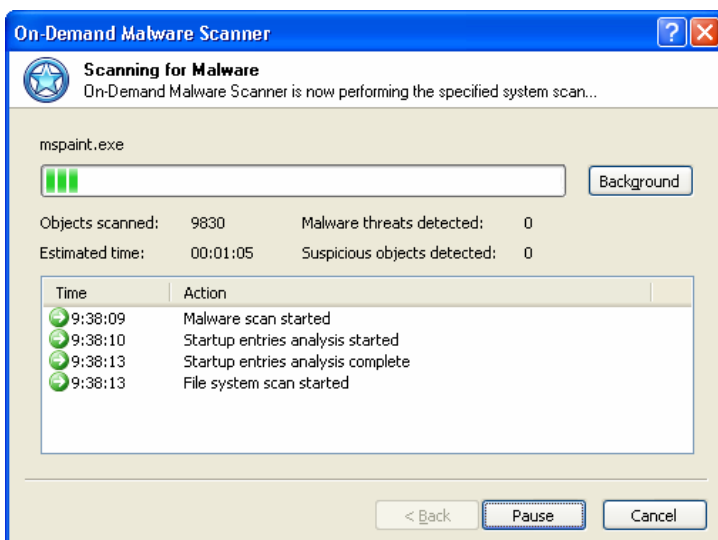
When you have specified the objects and locations to scan, click **Next** to start the [scan process](#).

Note:

- Spyware (a specific type of malware) cannot be cured and is automatically quarantined.
- The specified action does not affect critical objects and cookies. If a critical object or cookie is detected during scanning, no action will be taken and the **Specify Actions for Detected Objects** step will be displayed after the scan is finished as if the **List All** action were selected.
- Irrespective of the specified action, all malware activity is blocked immediately after it is detected.
- Outpost Security Suite Pro scans files contained in ZIP, RAR, and CAB archives.

8.1.3 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:



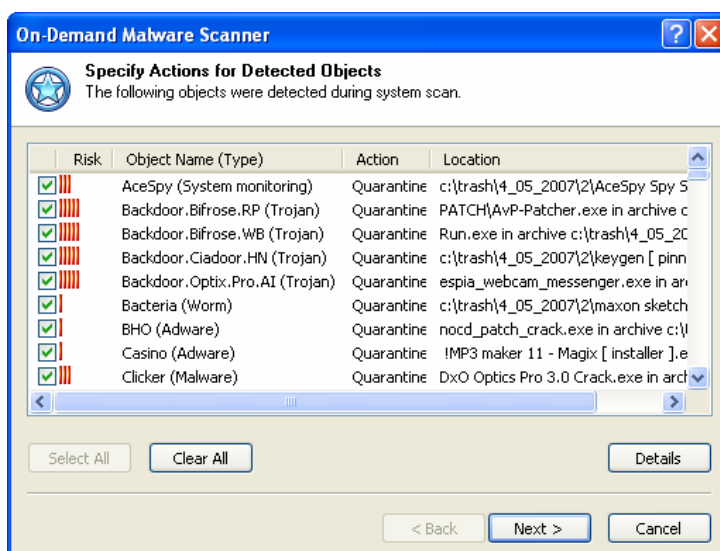
The scanning process can run in background mode. If you want to work with Outpost Security Suite Pro while the scan is underway, click the **Background** button and the wizard will be minimized. To see the full window again, select **Anti-Malware** on the left panel of the main window and click **Show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

8.1.4 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 malware quarantine, see [Malware Quarantine](#).

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

Tip:

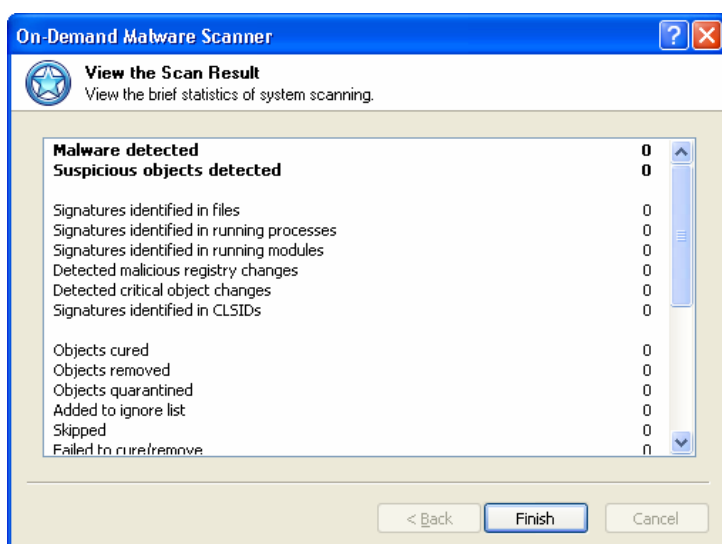
- If you know that a found program is not malware but is in fact legitimate software and do not want to treat it as spyware or a virus (for example, in order to use a freeware application, it must display its ads from a particular adware program), you can add such programs to the exclusions list. Outpost 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. To add a detected program to the exclusions list, right-click its name and select **Add to Exclusions**. You can also specify folders, which Outpost Security Suite Pro should not scan for malware. You can later remove programs and folders from the exclusions list 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).

8.1.5 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:



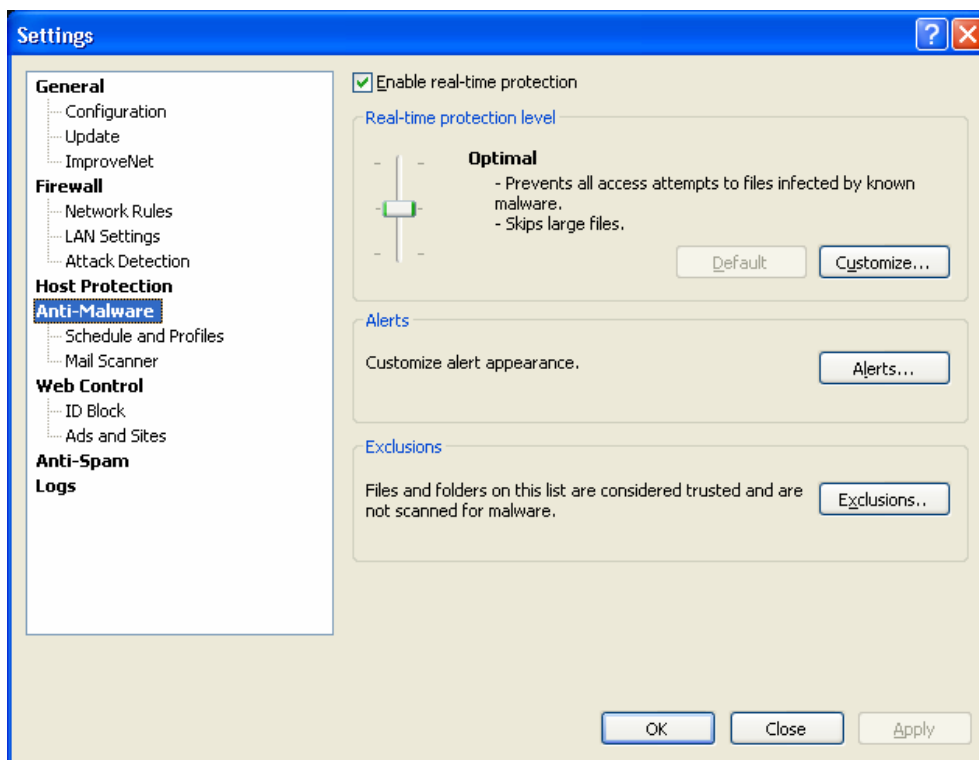
Note:

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.

8.2 Real-Time Protection

The Anti-Malware component provides real-time non-stop protection against spyware and viruses. When real-time protection is enabled, all system vulnerable objects are permanently monitored to ensure that malware is detected before performing any malicious activity.

To enable real-time protection, open the component properties by clicking **Settings > Anti-Malware** and selecting the **Enable real-time protection** check box:



There are three levels of real-time protection possible to select:

- **Maximum.** All access attempts to files infected by known malware are prevented. Embedded OLE objects are checked either. A heuristic method of finding new malware is used.
- **Optimal.** Files are checked when they are accessed. Files larger than 20MB are skipped.
- **Relaxed.** Particular types of executable files are checked only when they are executed. Files larger than 20MB are skipped.

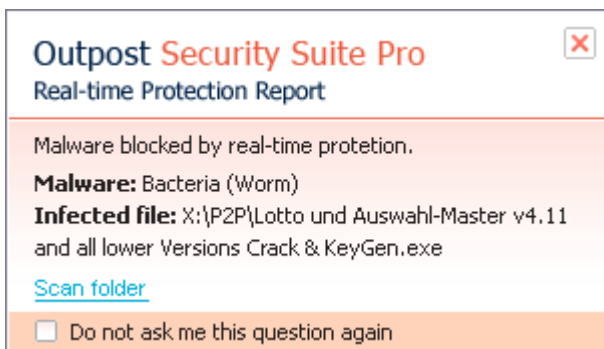
If you want to create your own real-time protection level, click the **Customize** button. In the dialog box you can set the real-time protection operation mode. Select **Check files on every access attempt**, which will prevent all access attempts to files infected by known malware. Note that this last mode can affect system performance. Or, you can select **Check files on execution**, if you want to prevent known malware from executing, but don't want to prevent other access attempts such as copying malware samples or displaying the contents of a folder where malware is located. Only file extensions that are on the **Extensions** list will be checked on any access attempt.

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.

On detecting a suspicious program, Outpost Security Suite Pro will block its activity and display an alert to the user that allows him to immediately scan the detected object for malware.

An alert looks like the following:



You can also set visual alerts to be displayed and/or sound alerts to be played when malware is detected by clicking the **Alerts** button and selecting the corresponding check boxes. Outpost Security Suite Pro will display a visual alert and play the specified sound file each time malware is detected and cured or quarantined. This lets you learn the programs you run and the sites you visit that are injecting malware or at the very least are susceptible to malware.

If you want to exclude particular folders from being scanned, click the **Exclusions** button on the **Anti-Malware** page, select the **Paths** tab and click **Add**. Browse to the folder and click **OK** to add it to the exclusions list.

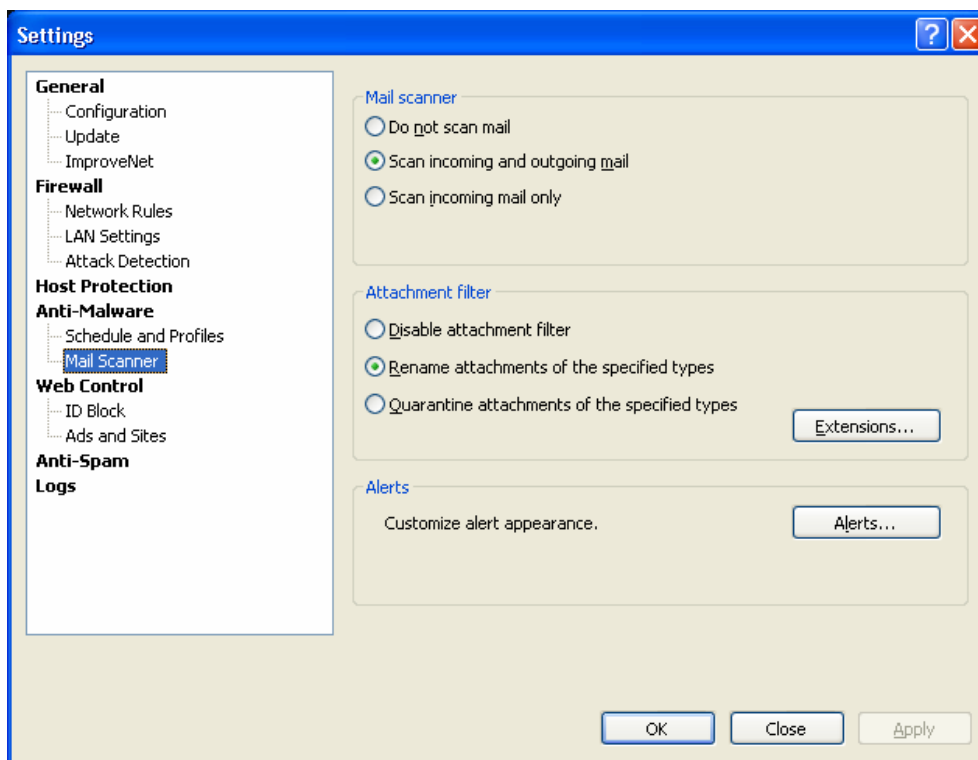
Note:

- To see the objects that the Anti-Malware component detected and removed, select the **Event Viewer** section in the main window and click the **Anti-Malware** log.

8.3 Scanning Mail Attachments

One of the simplest ways for worms, Trojans, and other malware to get into your computer is through e-mail attachments. Hundreds of self-replicating programs use e-mail and address lists of unlucky users to distribute themselves throughout the Internet and/or a local network. A user needs only to open the file attached to a received e-mail and the worm or virus starts performing its malicious actions resulting in system infection and malfunction.

Outpost Security Suite Pro protects you from attachments containing viruses, worms, and Trojans, checking files attached to e-mail arriving to and being sent from your computer and quarantining those which Outpost Security Suite Pro recognizes as potentially dangerous:



Mail scanner

To configure the mail scanner, click **Settings** on the toolbar and select the **Mail Scanner** page. Under **Mail scanner** you can select which mail will be scanned: both incoming and outgoing mail or incoming mail only according to your needs. Also specify the action to perform on malware that is detected in your e-mail by selecting **Cure** or **Quarantine** in the **When malware found** list.

If you do not want to check e-mail messages for viruses and other malware, select **Do not scan mail**.

Attachment filter

If you consider some types of attachments to be potentially dangerous even after they pass a clean malware check (for example, the scanner could simply be not "aware" of a new virus in the wild) or for some reason have disabled mail scanning, you still have the ability to prevent probable damage caused by opening or executing such a file.

The attachment filter is triggered after a clean malware scan quarantines or removes specified types of files according to the settings under **Attachment filter** on the **Mail Scanner** page.

Select **Rename attachments of the specified types** if you want to change the extension of the file or **Quarantine attachments of the specified types** to isolate them and put them in Outpost Security Suite Pro's quarantine.

To edit the list of file extensions to process, click the **Extensions** button. The most common types of files that can contain malicious code are already added to the list for your convenience, but you can add, edit, or remove file extensions according to your needs. To revert to the original list, click the **Default** button.

If you do not want the filter to rename or quarantine any attachments, select the **Disable attachment filter** option button.

You can also set Outpost Security Suite Pro to show visual alerts and/or play sound alarms on detecting malware by clicking the **Alerts** button under **Notifications**.

Note:

- Only IMAP, POP3, and SMTP protocols are supported. Outpost Security Suite Pro does not support Microsoft Exchange mail accounts.

8.4 Malware Quarantine

Outpost Security Suite Pro's default procedure for removed malware is to not delete it completely but to place it into a special isolated storage called *quarantine*, so it can be restored later if you find an application you depend on will not function without its associated malware. This will let you recover the data that the application uses, so you can then uninstall it and find another app that doesn't use spyware. Objects in quarantine do not pose any threat to your computer.

Quarantined objects are displayed in **Quarantine** in the main Outpost Security Suite Pro window. Every malware program and object is represented in the quarantine list only once despite the number of separate signatures detected. For each object quarantined, the date and time it was detected, and its location and type are displayed. If you highlight an object, you will see its description, and detailed information about the locations of all related objects in the **Detailed Information** below its description.

Each item quarantined as spyware can be restored from quarantine to resume its normal operation on your computer. To restore an item, click the **Restore** link next to it. (Registry keys and INI files will be restored to just before they were quarantined.) You can also restore an object and add it to the Ignore list to make Outpost Security Suite Pro ignore it as spyware by selecting the **Restore and Add to Ignore List** command on the item's shortcut menu.

For viruses and items quarantined by the attachment filter, you have the ability to save the object on your hard disk using the **Save As** command. This lets you view the file contents without damaging your system.

You can also permanently remove any object by clicking its **Delete** link. To delete all the quarantined objects, use the **Clear Quarantine** command on the shortcut menu.

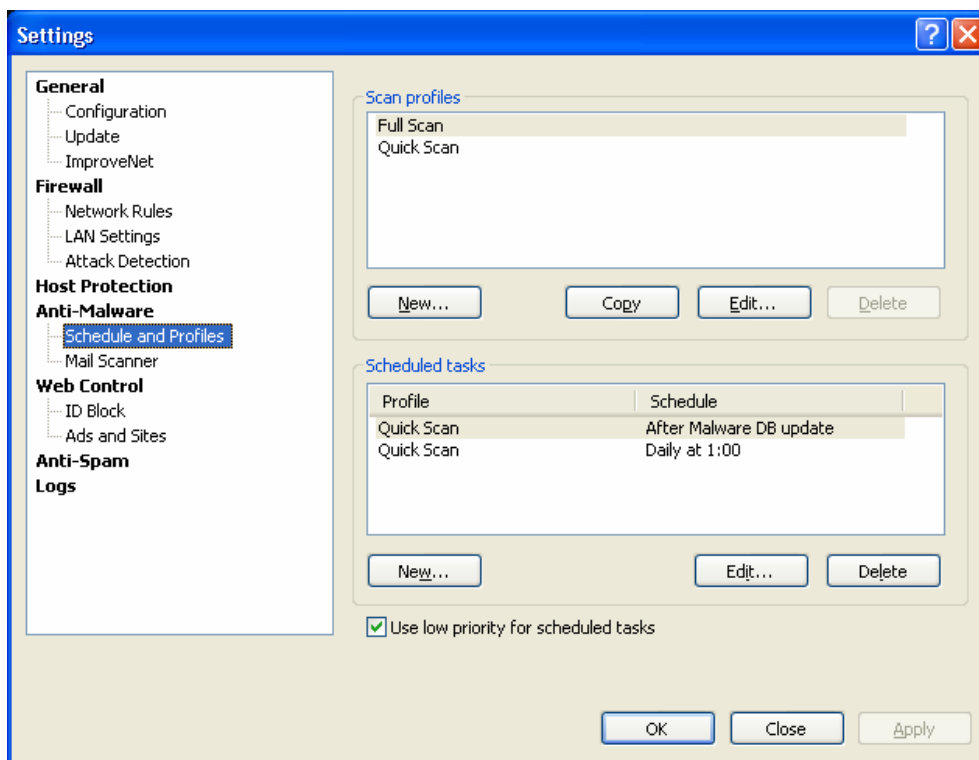
Note:

- There are some spyware programs that cannot be placed into quarantine. These are simply removed.

8.5 Scheduling System Scan

Scheduling a system scan is a very useful option if you want to save time and computer resources while scanning your system or if you need to perform regular scans. Outpost Security Suite Pro can perform scans in unattended mode when you are away of the computer.

To set a scheduled scan, click **Settings > Schedule and Profiles:**



By default, scheduled quick scans are performed after updating the malware database and daily at 1 a.m. To create a scheduled scan, click **New**. Enter a name for your task, select a scan profile to be used from the drop-down menu and specify the scan schedule. To create regular malware scans, use the **How often** list. If you select **Weekly** scanning, you can also specify the day and exact time when Outpost Security Suite Pro will scan your system. If you choose **Daily** scanning, you can specify the time of day for the scanning to begin.

To temporarily disable a scheduled task without deleting it, highlight it on the list and click **Edit**. Clear the **This task is enabled** check box. The profile is not permanently deleted, and later you can enable it again. To delete a profile completely, highlight it and click **Delete**.

To save system resources at a time when the computer performs critical activity, select the **Use low priority for scheduled tasks** check box.

Click **OK** to save the settings. Outpost Security Suite Pro will launch a system scan according to the specified schedule.

9 Controlling Online Activities

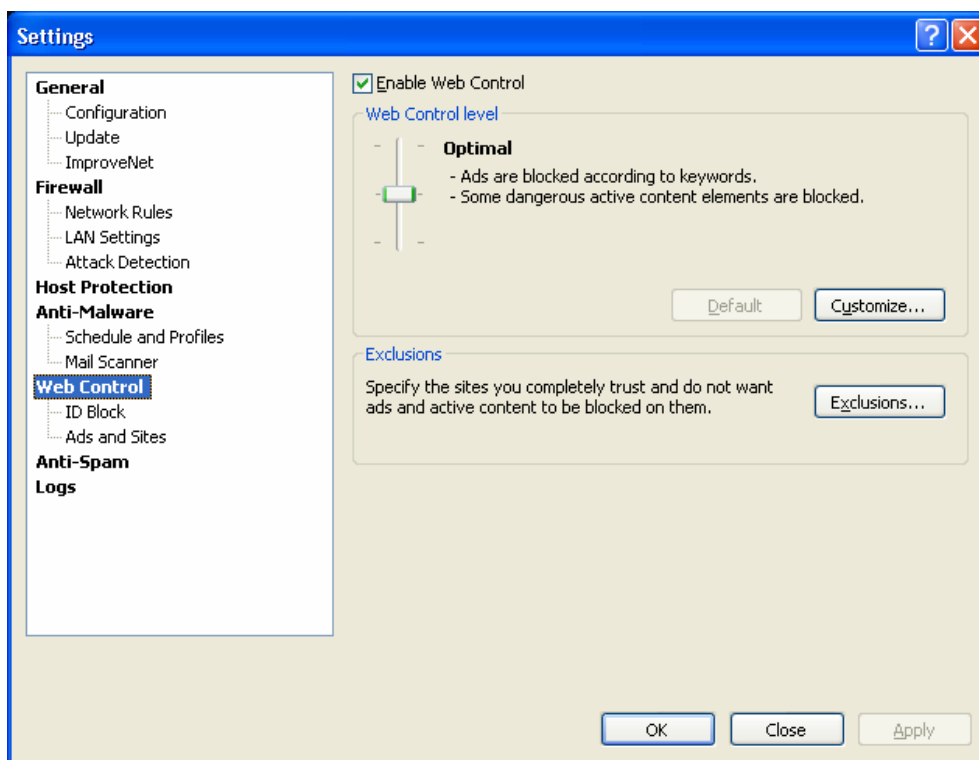
Contemporary web site developers embed active elements in web pages to extend their functionality, increase user interactivity and improve web site usability. These elements include ActiveX, Flash, JavaScript, VBScript, and others. These technologies were developed to improve the user experience as people browse web pages, but hackers are now successfully using them to gain control of your computer. Active elements can pose a security risk to your system. Many sites also use them to display obtrusive, offensive or simply annoying ads, which can significantly decrease browsing speed.

Besides, more and more web sites are full of banner ads that often are very irritating, clutter up web pages with objectionable images and which can practically stop already slow modem browsing.

Outpost Security Suite Pro's Web Control component provides Internet surfing safety. It controls the operation of active elements embedded in the web pages you are browsing or in the e-mail you are receiving so you can independently allow or block any of these elements. The following are controlled by this plug-in: ActiveX, Java applets, programs based on Java and Visual Basic scripts, cookies, pop-up windows, ActiveX scripts, external active content, referrers, hidden frames, animated GIF images, flash animations.

Web Control also blocks the display of banner ads from specific advertisers, which speeds up web pages. Advertisements can be blocked using two criteria: by keywords found in the content of the downloaded web page or by the size of the ad image.

To enable protection from such unnecessary ads and active content, click **Settings > Web Control** and select the **Enable Web Control** check box:



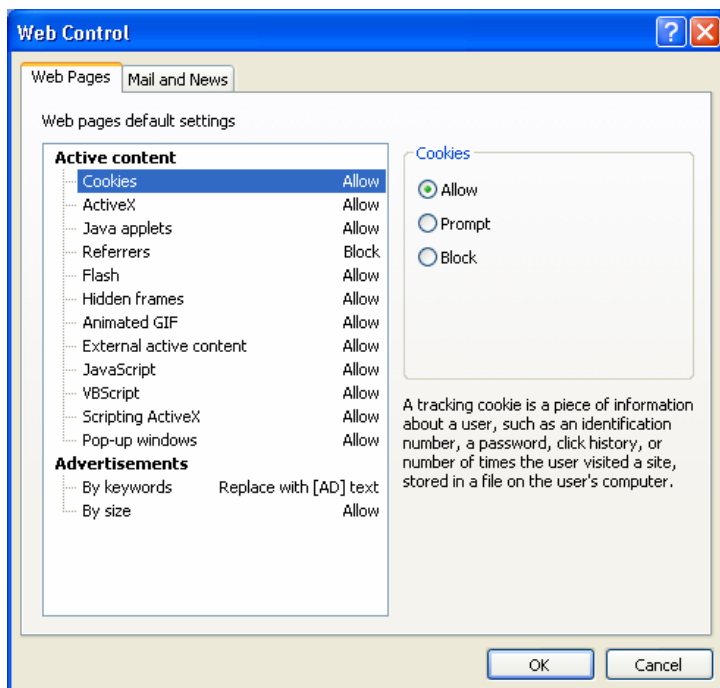
9.1 Setting Web Control Level

You can specify how thorough Outpost Security Suite Pro should be in processing web content by changing the Web Control level. To change the Web Control level, click **Settings** on the toolbar and select the **Web Control** page. The following levels are available:

- **Maximum.** Advertisements are blocked according to specified keywords and sizes. The most dangerous active elements are blocked or cause a prompt to be displayed to a user.

- **Optimal.** Ads are blocked according to specified keywords and most active content elements are allowed.
- **Relaxed.** Ads are blocked according to specified keywords and all active content is allowed.

If you want to define special settings, you can customize the protection level. Click the **Customize** button and the displayed window will let you independently configure the treatment of interactive elements and ads contained in downloaded web pages or your e-mail and news:



Go to either the **Web Pages** or the **Mail and News** tab and select the element type to manage. The right part of the window will show you the element description and the setting for each selection. To allow or block a particular element, select one of the available options:

- **Allow.** All elements of this type are always allowed.
- **Prompt.** Outpost Security Suite Pro prompts you before allowing an element of this type.
- **Block.** Elements of this type are always blocked.

For advertisements, Outpost Security Suite Pro gives you the option to either replace banner ads with text "[AD]" or with a transparent image the same size as the banner. Note that although replacing banner ads with transparent images greatly increases your comfort level while browsing by removing annoying graphics, you may prefer to replace banners with the "[AD]" text links so you can still use the links if you like.

Click **OK** to save the new settings.

The **Default** button restores the default protection level.

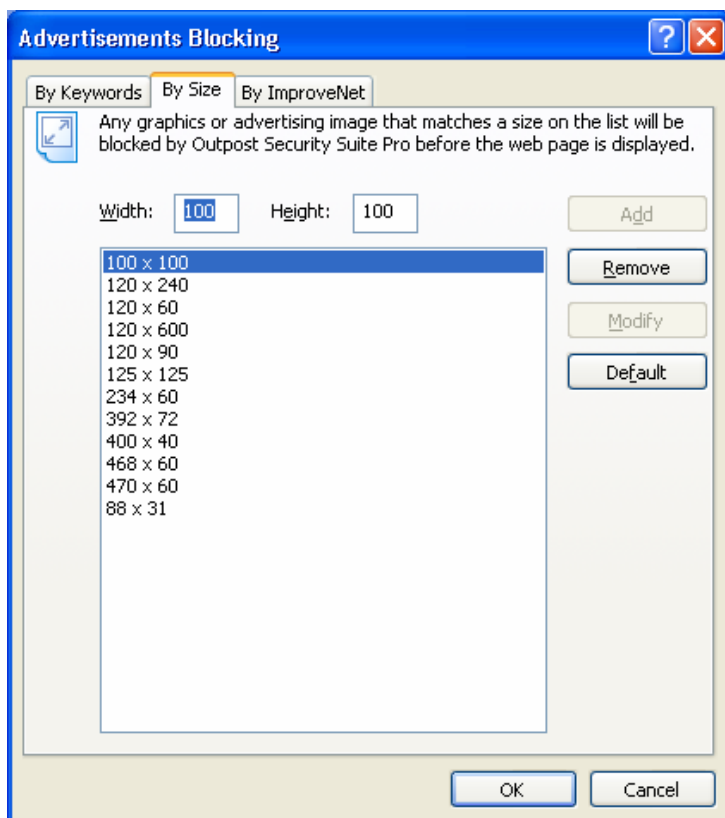
Note:

- The **Prompt** option is not available for hidden frames, animated GIFs, and external active content.
- Some sites require that all or several of its active content elements be active for their pages to display or function correctly. If you make the settings for all sites very restrictive, you can experience the following problems: necessary images not being displayed, a web page not showing at all, a web page displayed incorrectly or some useful services contained in applets not working. If this happens with only a few regularly visited sites, just change these settings for

those sites by adding them to the [exclusions list](#); otherwise you may need to loosen the default web content treatment policy.

9.2 Advertisement Blocking

Advertisements can be blocked using the following three criteria: by keywords found in the content of the downloaded web page, by size of the advertising image and using the data collected via the [Agnitum's ImproveNet](#) program:



Blocking by keywords

Outpost Security Suite Pro blocks ads basing on keywords found in Internet advertisement URLs located in the "*IMG SRC=*" and "*A HREF=*" HTML tags. If the banner URL contains one of the specified keywords, it is replaced with the text "[AD]" or with a transparent GIF image the same size as the ad image.

To open the component's list of keywords, click **Settings > Ads and Sites > Edit List**. To add a word to the blocked list, type it in the provided text box and click **Add**. The word will appear in the list and any advertisement that contains this word, will not be displayed in the web browser. You can also edit and remove keywords from the list.

You can also import and export lists of keywords by using the corresponding buttons.

Blocking by image size

Outpost Security Suite Pro blocks advertisement images based on their size as specified within the "*A*" HTML tag. If the banner size matches one of the sizes on the list, it will be replaced with the text "[AD]" or with a transparent GIF image of the same size.

By default, the standard size ad images are already on the list. To block a banner with a different size, click **Settings > Ads and Sites > Edit List**, select the **By Size** tab and specify the banner's width and height in the fields provided and click **Add**. The size record will appear in the list and any ad of this size

will not be displayed in the web browser. You can also edit and remove sizes from the list. To reset the list to its default state, click the **Default** button.

Blocking by ImproveNet

This function is similar to "blocking by keywords" with the difference that the keywords in ImproveNet *are shared by users of Outpost Security Suite Pro*. The list of ImproveNet keywords is automatically updated along with the regular product updates either automatically (if that is your preference) or manually. You can also contribute to the ImproveNet program if you find a word on the list that you believe should not be on the shared list of keywords. To do this, select the word in the list and click the **Report an objectionable word** link at the bottom of the page.

Blocking by ImproveNet is an optional function, therefore if you do not need it you can disable it by clearing the **Use ImproveNet ads keyword list** check box on the **By ImproveNet** tab.

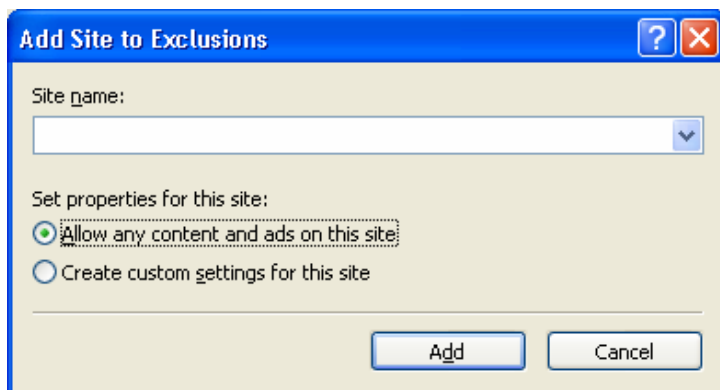
Note:

- Banner ads are blocked according to the settings you specify. Therefore, some legitimate images could be blocked if a setting is too broad, such as adding the word "image" to the list of keywords. At the same time, some ads might not be blocked with the component's default settings.

9.3 Specifying Exclusions

If you experience problems viewing specific sites because most of the site's images are filtered out, you can add those sites to the exclusions list and set the policy for handling active content elements and ads individually for that particular web site to stop the component from being blocked.

Click **Settings > Web Control > Exclusions** and click **Add** to specify the address of the site you want to personalize the content settings for:



You can either **Allow any content and ads on this site** making it completely trusted or specify your individual settings by selecting the **Create custom settings for this site** option. In the second case, after clicking **Add** the **Edit Properties** window for this site will be displayed allowing you to set how the site's active content and ads should be treated. The site that you add is immediately given all the default active content and advertisement settings for the current Web Control level. The settings are pretty much the same as the [global settings](#) for all sites. The only difference is that you can select **Use global setting** (for the active elements—instead of the **Prompt** action) for the element behavior to be defined by the global setting (displayed in brackets) for this site.

Note that settings that inherit global values are displayed in **gray**; settings that are assigned unique values are displayed in **blue**. Make your choices (use the **Default** button if you want to start from the global settings again) and click **OK** to save your changes.

You can later edit the site's active content and ad settings by selecting the site from the list and clicking **Properties**.

9.4 Site Blacklist

Various sites on the Internet contain spyware and they aim at spreading it among unwitting users. Outpost Security Suite Pro's database contains a list of such sites, access to which is not recommended unless you are eager to load spyware on your system on purpose. An attempt to make a connection to such site or to send any data there is automatically blocked. The full list of these sites is invisible to users, but on detecting an attempt to access one of these sites, Outpost Security Suite Pro adds it to the visible list, which is available by clicking **Settings > Ads and Sites** and clicking **Settings** under **Site blacklist**.

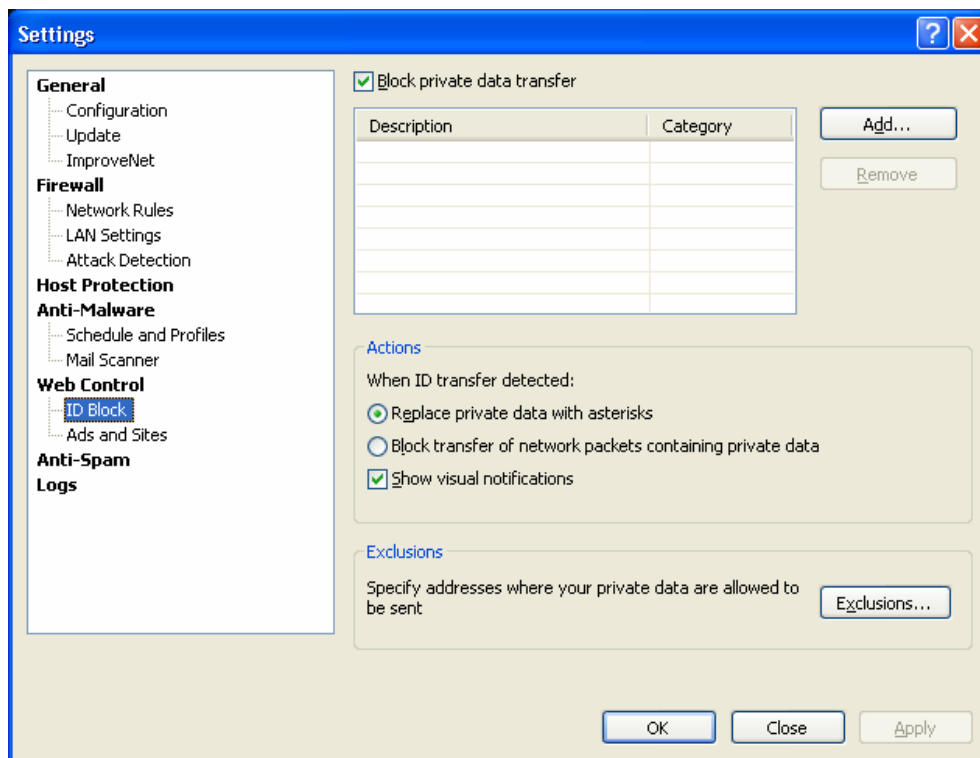
If there are any sites that you use or consider safe, you can allow access to them by clearing the corresponding check boxes.

To be aware of spy site blocking, you can set Outpost Security Suite Pro to display alerts by selecting the **Show visual notifications** check box.

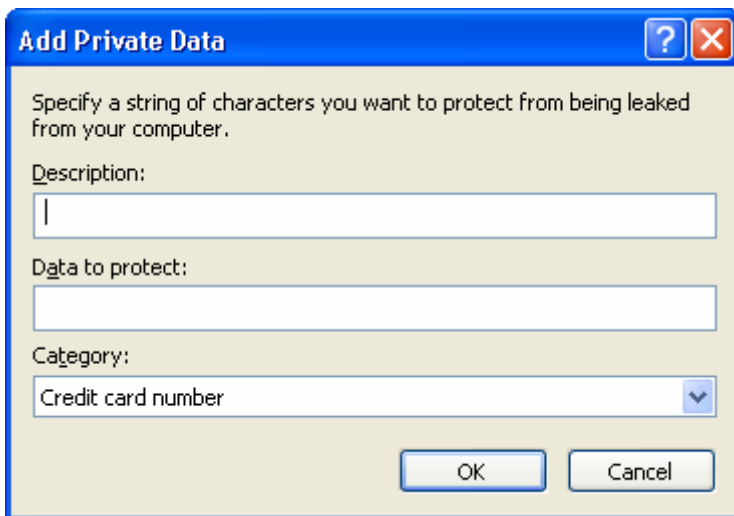
9.5 Blocking Private Data Transfers

Outpost Security Suite Pro lets you specify your personal data that should never to be transmitted by your computer through Internet browsers, instant messaging software, e-mail clients or any other application. This provides protection against identity theft through abuse of credit card account details, passwords, or other unique and valuable personal information.

To protect your private data, select the **ID Block** page of the **Settings** window and select the **Block private data transfer** check box:



Click **Add** and in the **Add Private Data** window specify the following parameters:



- **Description.** This is a description that you will be able to recognize later to identify the string.
- **Data to protect.** Any combination of symbols, letters or digits you do not want to leave your computer.
- **Category.** The category your data belongs to.

After clicking **OK** and applying the changes, that string will be blocked from any outgoing communication.

On detecting a private data transfer, Outpost Security Suite Pro can either **Replace transferred ID with asterisks** or **Block transfer of network packets containing private data**. In the first case, any requesting source will receive only asterisks in place of the data while in the second any attempts of a requesting source to get data will be completely blocked.

To have alerts displayed each time an attempt is made to transfer one of the specified strings from your computer, select the **Show notification when private data transfer is blocked** check box.

If you are certain that some hosts are trustworthy or they need to receive your private data, you can add such hosts to the exclusions list by clicking the **Exclusions** button. Specify the necessary site in the most convenient format for you, click **Add** and **OK** to save your settings.

10 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.

10.1 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.

10.2 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.

10.2.1 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.

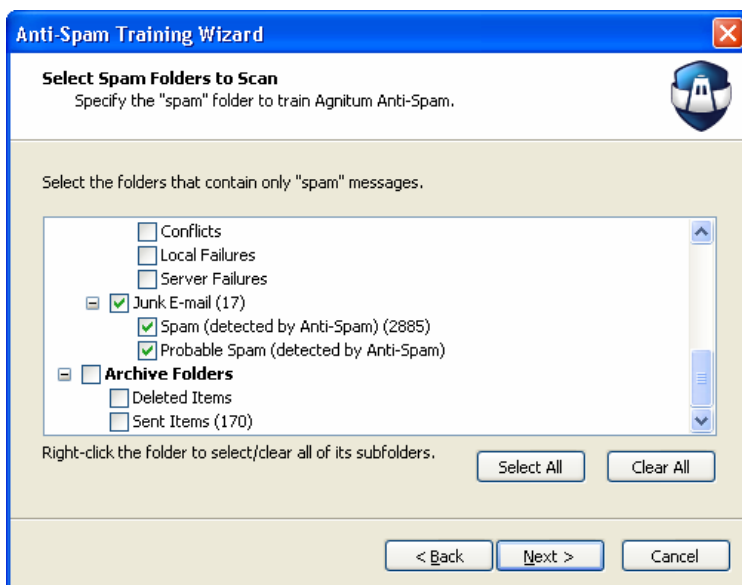
Important:

- 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.

10.2.2 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.

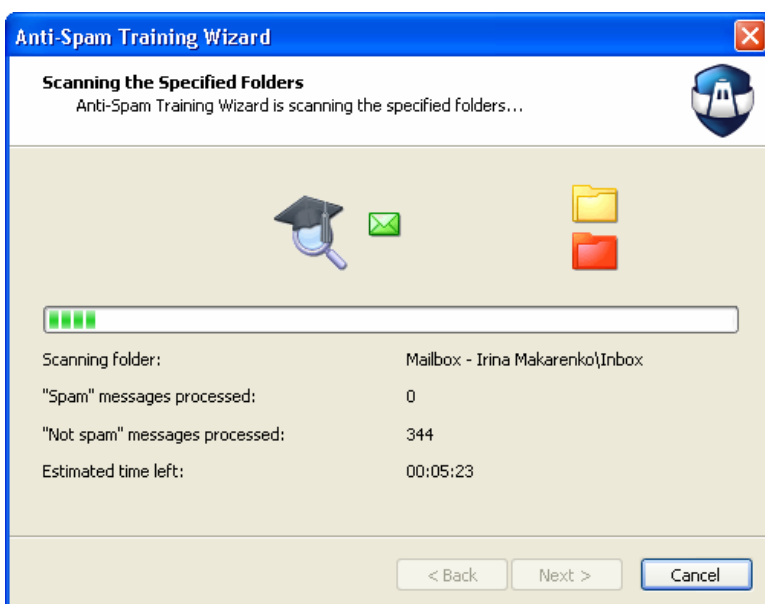
Tip:

- 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.

10.2.3 How Does the Bayesian Filter Work?

Each word has a probability of occurring in spam e-mail (which is specific to each user). For example, most users will frequently encounter the word "Viagra" in spam messages, but will rarely see it in good messages. Anti-Spam doesn't know these probabilities in advance, and needs to be trained to compute them. To train the filter, you (manually or automatically, using the training wizard) specify whether a particular message is spam or not. For each word in each training message, Anti-Spam calculates the probability that it will appear in a spam message (this is what we call "rank") based on the times it occurs in messages marked as "spam".

All the probabilities are saved in Anti-Spam's knowledge base, which changes as Anti-Spam gains experience. For example, Anti-Spam will most likely assign a high ranking to the word "Viagra", but a low ranking to words found only in legitimate messages, such as the names of your friends.

The rank is recorded as a decimal number in the range of 0 to 1. A neutral rank value (0.5) shows lack of any definitive estimate. Words with a rank close to the neutral value are of little interest for the overall probability that the message is spam, so have a low "weight". On the contrary, those with a rank much higher or lower than 0.5 are definite indicators (have a high "weight") that the message is spam or not, respectively. A word's weight simply means that it has some influence on a message being labeled as spam or not spam.

The probability that a message is spam (an overall message rank) is computed using the rankings of all the non-neutral words in the message (words with weight) based on Bayes' theorem and is a number in the range of 0 to 100. Zero means definitely not spam and 100 means definitely spam. If the message rank exceeds a specified threshold (by default, 85 for the **Normal filtering level**), Anti-Spam marks the message as spam.

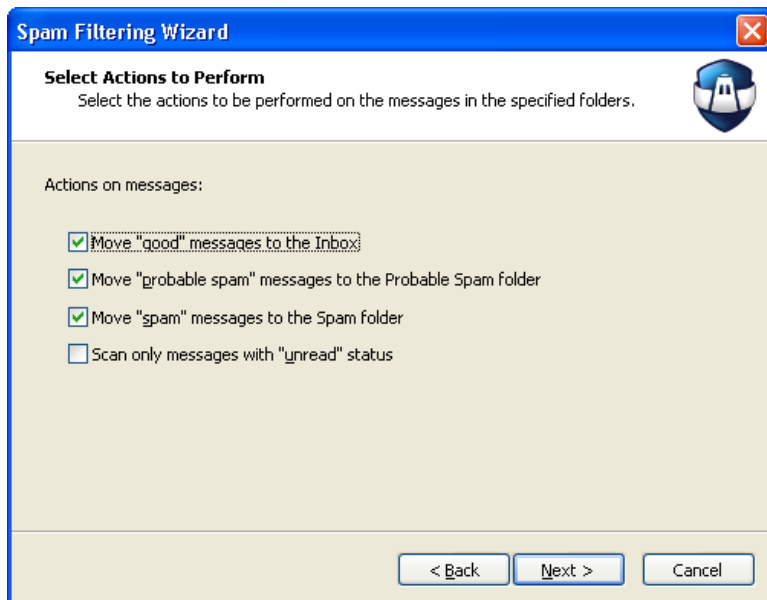
After Anti-Spam is trained, you can view the spam statistics for each message by clicking the **E-Mail Details** button on the toolbar. The **Filtering Details** window displays the message status and its rank, as well as the words used to calculate the message rank with their spam probabilities and weight. Note that these statistics are relevant only for the current moment, not at the moment the message was received.

10.3 Scanning Mail Folders

You can use Anti-Spam to clear the existing message collection from spam, or to filter out good messages from folders flooded with spam, which can be quite tedious if done manually.

Click **Agnitum Anti-Spam** on the plug-in toolbar in your mail client and select **Scan Folders** on the drop-down menu to start the **Spam Filtering Wizard**. The wizard will prompt you to select folders to scan (the same way you did in [Anti-Spam Training Wizard](#)). After selecting the folders, click **Next**.

The second step of the wizard allows you to select the actions you want to be performed on messages in the selected folders:

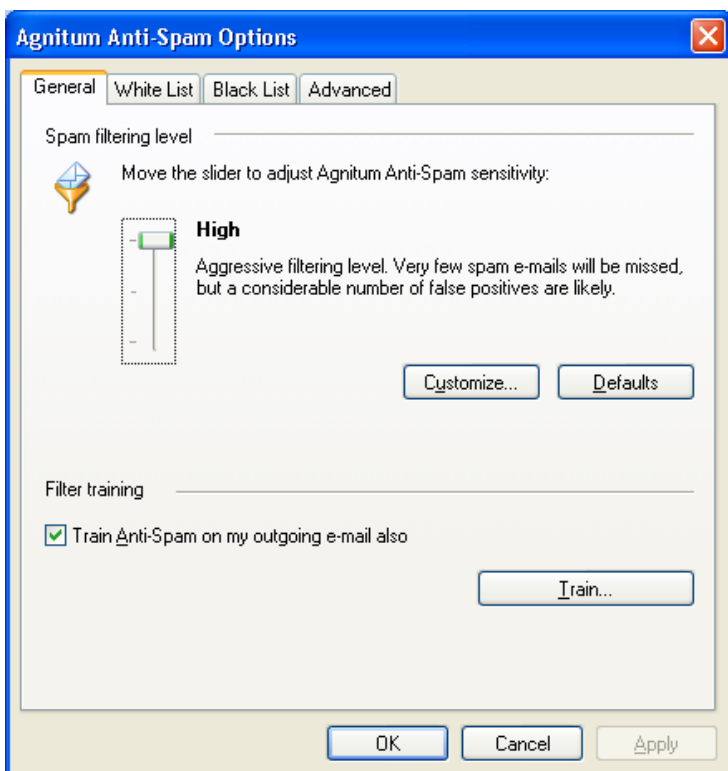


If you want to filter out good messages from these folders, select the **Move "good" messages to the Inbox** check box. To clear these folders from spam messages, select the check box labeled: **Move "spam" messages to the Spam folder** (and optionally **Move "probable spam" messages to the Probable Spam folder**). If the **Scan only messages with "unread" status** check box is selected, Anti-Spam will process only "unread" messages (for example, new messages received during the last session).

After specifying the required actions, click **Next** to start processing. After the processing is complete, click **Finish** to close the wizard.

10.4 Setting the Filtering Level

The filtering level defines how aggressive Anti-Spam is in filtering spam. To set the filtering level, open Anti-Spam's settings by clicking **Agnitum Anti-Spam** on the component toolbar in your mail client and selecting **Options**. Move the slider on the **General** tab to change the filtering level:



The following three levels are available:

- **High.** Provides the most aggressive filtering, the probability of missing spam is minimal, but a considerable number of false positives (legitimate messages labeled as spam) is possible.
- **Normal.** Provides optimal filtering, most spam messages are detected with the minimum number of false positives.
- **Low.** Provides light filtering that rarely gives false positives, but allows some spam messages into the Inbox.

To customize the filter sensitivity to better match your requirements, click **Customize:**



In the **Spam Filtering Level** window, you can set the precise rank according to which messages will be filtered. Moving the sliders, specify the rank value the message must obtain to be treated as the "spam" and "probable spam". To save the settings, click **OK**.

To restore the default filtering level, click **Default**.

Tip:

- Anti-Spam puts the message status (spam/not spam) and its rank (calculated at the moment the message was received) in the message header, for example:

X-Agnitum-antispam: SPAM

X-Agnitum-antispam-rank: 99

You can use this information to collect statistics or configure the filter more flexibly.

10.5 Specifying White and Black Lists

White and Black lists are meant to automatically correct the behavior of the Bayes method in cases where it systematically treats some specific type of messages incorrectly. In this case you can create a corresponding White or Black list rule manually and on receiving the next difficult message, the filter will rank it and mark it according to that rule.

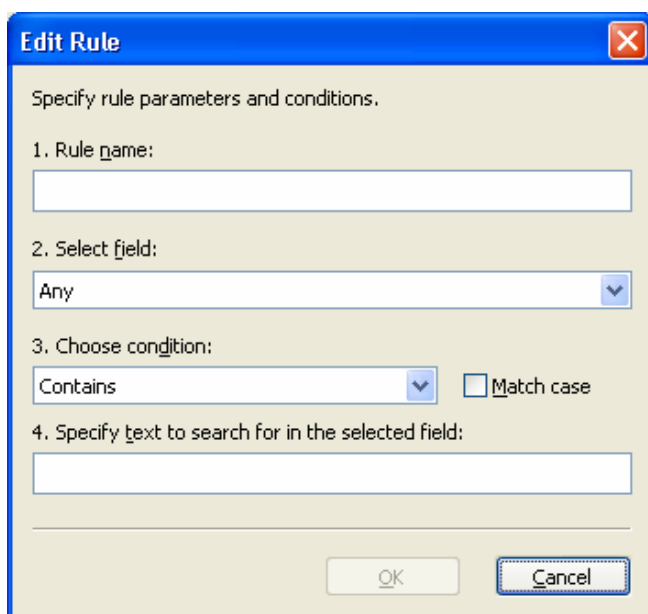
List filtering has a higher priority than the Bayes method. This means that if the message meets the conditions of one of the specified White or Black list rules, it will be ranked according to that rule irrespective of the Bayes rank and Anti-Spam will automatically mark it as "spam" or "not spam".

White and Black lists help to prevent accidental false positives (legitimate e-mail misidentified as spam).

White list (**Options > White List**) rules define those messages that never should be considered as spam. Any message satisfying the conditions of one of the white list rules (e.g. matching e-mail address, IP address, and domain name or containing the specified keyword) is directly marked as "not spam" and always allowed into your Inbox. White list rules have the higher priority than black list rules.

Black list (**Options > Black List**) rules let you create rules for messages you do not want to receive. Any message satisfying the conditions of one of the black list rules (e.g. matching e-mail address, IP address, and domain name or containing the specified keyword) is automatically marked as "spam" and moved to the **Spam** folder. Anti-Spam is also trained on these messages (information is added to the knowledge base).

The configuration and editing of both lists is similar. To add a new rule, click **Add**:



In the **Edit Rule** window, you can specify the rule's parameters and conditions by following these steps:

1. Rule name

Specify the rule name that will be displayed in the list. If you leave the text box blank, the name will be calculated automatically based on the rules parameters. The rule name does not affect the action of the filter.

2. Select field

Use the **Choose field** drop-down list to specify the field of the message to be searched. The following fields are available:

- **Any**—the whole message as it was received.
- **Header**—message service headers.
- **Subject, From, To, Cc, Bcc**—contents of the message fields of the same name.
- **Body**—message body except the headers.

3. Choose condition

Use the **Choose condition** drop-down list to specify the way to match the specified text with the specified field contents. If you want to enable a case-sensitive search of the specified text, select the **Match case** check box. The following conditions are available:

- **Contains/Does not contain**—simply searches for the specified text in the specified search field.
- **Starts with/Does not start with**—matches the required text at the beginning of the specified search field.
- **Ends with/Does not end with**—matches the required text at the end of the specified search field.
- **Equals/Does not equal**—checks whether the required text completely matches the specified search field.
- **Matches/Does not match**—considers the specified text as a regular expression and checks whether the specified search field satisfies this expression.

4. Specify text to search for in the selected field

Specify the required text. This can either be an e-mail address, a simple keyword contained in the message, or a regular expression (if the **Matches/Does not match** condition is used).

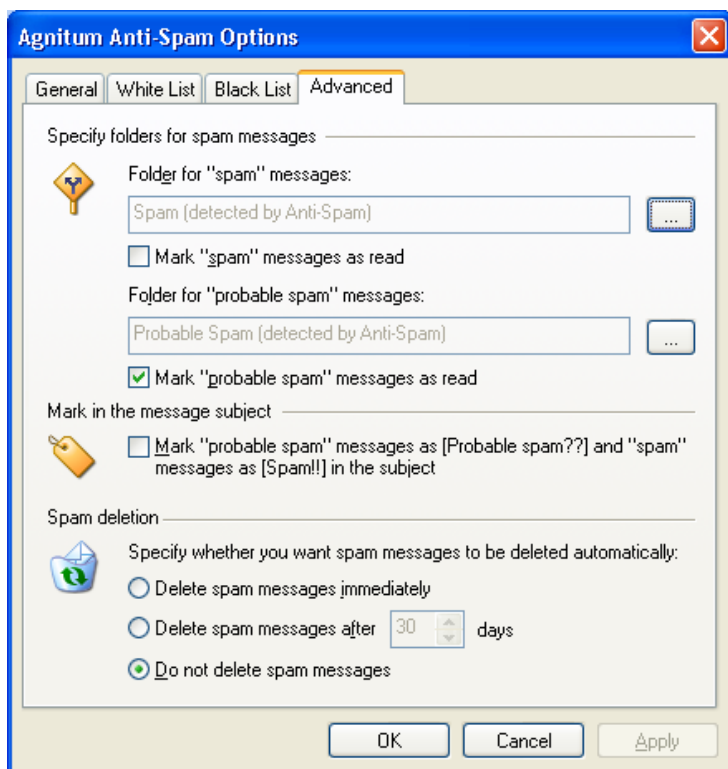
After specifying all the parameters, click **OK** to save the rule.

To edit a selected rule, click **Edit**. To delete a selected rule, click **Remove**. To copy a selected rule, click **Copy**.

You also have the ability to specify contacts to which you write and names in the **Contacts** list in your mail client, as trusted recipients. On the **White List** tab, select **Automatically allow e-mail from people I write to** and/or **Automatically allow e-mail from addresses on my Contacts list** and Anti-Spam will automatically allow e-mail received from these addresses.

10.6 Specifying Additional Settings

On the **Advanced** tab of the **Options** dialog you can specify some additional Anti-Spam settings:



Specifying folders

By default, **Spam (detected by Anti-Spam)** and **Probable Spam (detected by Anti-Spam)** folders are automatically created in your **Inbox** folder (in Microsoft Outlook 2003, in the **Junk E-mail** folder) to which Anti-Spam sends letters ranked as "spam" and "probable spam". But you can specify alternate folders to receive spam and "probable spam". Click the corresponding ellipsis button to modify the folder. Select the folder in the standard mail client window displaying all folders in your mail database and click **OK**. Note that any folders currently containing spam will not be affected; all newly detected "spam" or "probable spam" messages will be moved to the newly specified folders.

You also have the ability to automatically mark moved letters as "read" if you select the corresponding check box.

Marking the message subject

For clarity, you can set Anti-Spam to mark the subjects of messages it detects as "spam" and "probable spam". To do this, select the **Mark "probable spam" messages as [Probable spam??] and "spam" messages as [Spam!!] in the subject** check box.

Spam deletion

If the amount of received spam is extremely large, you might want to periodically clean your spam folders to save the disk space. Anti-Spam allows you to perform this task automatically by providing **Spam deletion** settings.

If you are confident that Anti-Spam is sufficiently trained and no legitimate messages are being labeled as spam during spam filtering, then you can set to delete spam immediately (rather than moved to a spam folder) by selecting the **Delete spam messages immediately** parameter. You definitely should not do this until you are sure you have Anti-Spam trained well.

If you need time to periodically look through your spam folder in order to reveal false positives and are afraid of missing some useful information, select **Delete spam messages after ... days** and specify the

number of days to keep spam. The aged spam will be deleted from the **Spam** folder after being kept the specified number of days.

You can also disable automatic spam cleaning by selecting the **Do not delete spam messages** parameter.

Important:

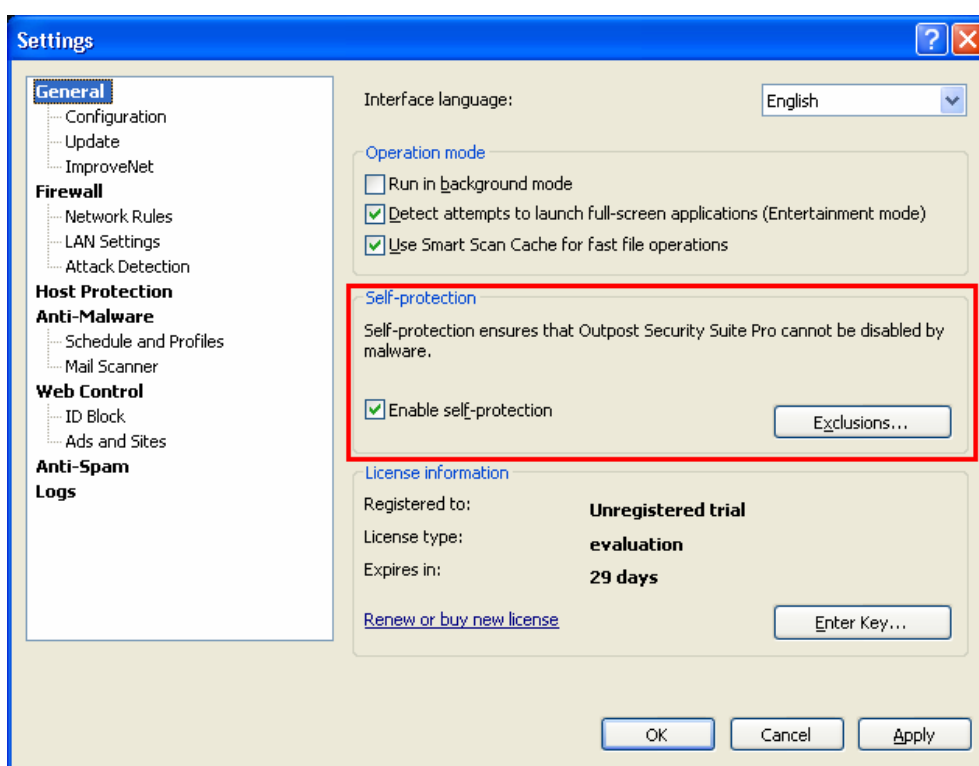
- Please note that during spam deletion, messages in the **Spam** folder are deleted regardless of their status. If this folder contains any good messages, they will also be destroyed; no folder rescan is performed before deletion.

11 Protecting Internal Components

As anti-malware tools have grown stronger, hackers now try to switch them off using rootkits and other advanced tools before proceeding with their own unauthorized actions. To withstand this threat, Outpost Security Suite Pro features self-protection. With self-protection turned on, Outpost Security Suite Pro protects itself against termination caused by viruses, Trojans or spyware. Even attempts to simulate user keystrokes that would otherwise lead to firewall shutdown are detected and blocked. Outpost Security Suite Pro also constantly monitors its own components on the hard drive, the registry entries, memory status, running services, and so on, and disallows any changes to these by malicious applications.

By default, self-protection is enabled and access to components is forbidden for all applications. If you consider that some applications should access Outpost Security Suite Pro's components and registry keys, you may add such applications to the exclusions list by clicking **Settings > Exclusions**.

To disable self-protection, click **Settings** and clear the **Enable self-protection** check box or right-click the Outpost Security Suite Pro icon in the system tray and select **Disable Self-Protection**:



Note:

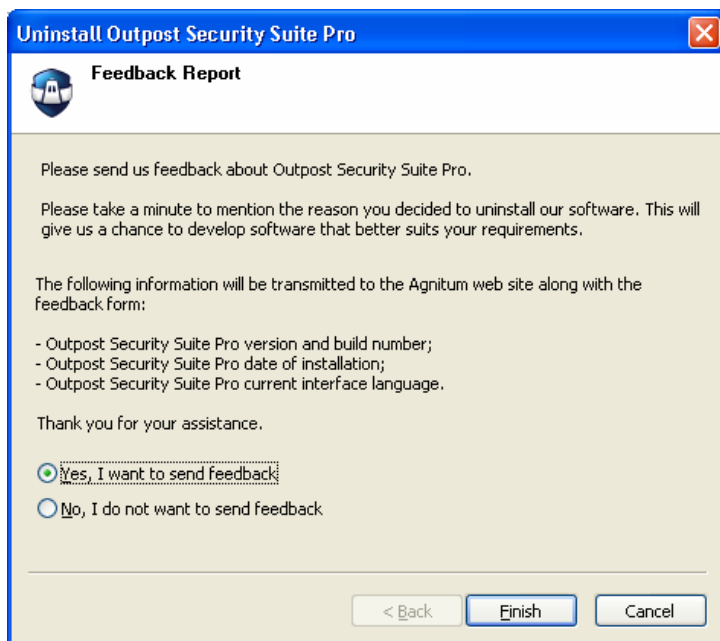
- Disabling self-protection may severely impact your overall system security. Though disabling is required for the installation of plug-ins and other advanced functions, it should be re-enabled as soon as the changes have been made.

12 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.

13 Tracking System Activity

For your convenience all system actions and events occurring on your computer are logged in detail and can be viewed using the Event Viewer, which shows every application and connection that was allowed or blocked by Outpost Security Suite Pro, as well as the specific activities of each Outpost Security Suite Pro component, the start of each program and all changes made to policies, configuration settings and passwords.

As distinct from the **Network Activity** log, which shows live connections and their details, the Event Viewer displays detailed statistics for all past system and product activities by category representing the history of events that occurred during the current Outpost Security Suite Pro session.

The Event Viewer is accessed by double-clicking **Event Viewer** in the left panel of Outpost Security Suite Pro's main window. By default, the following logs are available (click the log name in the left panel to view the specific data stored in that log):

- **Product Internal Events**

This is a record of program starts and shutdowns, the status of its components, and every change made to policies, program options and configuration settings.

- **Firewall**

Displays all the connections that Outpost Security Suite Pro has allowed or blocked and the reason why. For information about the Firewall component, see [Managing Network Connections](#).

- **Attack Detection**

Displays each suspicious activity and attack on your computer from the Internet and local networks, the ports involved and where the attacks are from. For information about the Attack Detection component, see [Preventing Network Attacks](#).

- **Web Control**

Displays all the interactive web page elements that were allowed or blocked based on the settings for Java, VB Script, ActiveX and other active content elements, advertisements, and malicious web sites or pages that were blocked by the Web Control component. For information about this component, see [Controlling Online Activities](#).

- **Anti-Malware**

Displays information about system scans and lists each virus and spyware that were detected and cured or quarantined from your computer. For information about the Anti-Malware component, see [Protecting against Malware](#).

You can also enable additional logs based on the information you need to track. To do this, click **Settings** on the toolbar, select the **Logs** page and select the **Show advanced logs** check box. The following additional logs will be available in the left panel:

- **System Events**

Displays the events of Outpost Security Suite Pro's Anti-Leak Control. For information, see [Controlling Penetration Techniques](#).

- **Packet Log**

Displays all the packets sent or received by the system and the reason they were allowed or blocked. For information, see [Managing Network Connections](#).

- **Component Control**

Displays all the events of Outpost Security Suite Pro's Component Control. For information, see [Controlling Application Components](#).

- **Anti-Leak Control**

Displays the events of Outpost Security Suite Pro's Anti-Leak Control. For information, see [Controlling Penetration Techniques](#).

Tip:

- Log files can be viewed manually using any text editor. To access the log files, click **Open Logs Folders** on the **Logs** page of the product settings.

13.1 Logging Level

To be able to get more information about your system's activity in case you encounter some issues with how specific applications perform, you can increase the depth of logging of firewall events or even enable logging of debugging information which can be useful for Agnitum's technical support service engineers to be able to resolve your issues.

Firewall logging level

To set the detail of firewall logging, use the settings available by clicking **Settings** on the toolbar, selecting the **Logs** page and clicking **Logging Level**. You have the ability to set the level of your global system logging and of application events, as well as low-level events.

Logging debugging information

To enable the logging of additional debugging information that is required for Agnitum's technical support service, click **Settings** on the toolbar, select the **Logs** page and select the **Log debugging information** check box. This will extend the number and detail of logged events.

You can modify the detail of which debugging information is logged by changing its logging level from 1 to 4. For the level change to take effect, you need to restart Outpost Security Suite Pro.

Note:

- Increasing the logging level may reduce system performance.

Tip:

- The size of each log can be limited to prevent log overgrowth and to save your hard disk space. On the **Logs** page, under **Log settings**, you can specify a size limit for every log in kilobytes.

14 Appendix

This appendix contains several technical topics, which can be useful for advanced users to be able to better understand Outpost Security Suite Pro's internals.

14.1 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.

14.2 Understanding Penetration Techniques

By means of [Anti-Leak Control](#), Outpost Security Suite Pro allows you to control the following actions:

Components injection

Windows operating systems by design enable installing system interceptors (hooks) through which foreign code can be injected into processes. Normally, this technique is used to perform common, legitimate actions, such as switching the keyboard layout or launching a PDF file within the web browser window. However, it can also be used by malicious programs to embed harmful code and thus hijack the host application. An example of a leak test that uses such a technique to stage a simulated attack is the PC Audit program (<http://www.pcindernetpatrol.com/>).

Outpost Security Suite Pro controls the installation of a hook interceptor in a process's address space. This is implemented via the interception of functions that are typically used by malicious processes (Trojans, spyware, viruses, worms etc.) to implant their code into legitimate processes, such as Internet Explorer or Firefox. The behavior of a DLL file invoking such functions is considered suspicious and triggers a legitimacy verification.

Control over another application

DDE technology is used to control applications. Browsers are commonly DDE servers, so can be used by malicious programs to transfer private information onto a network. One example of this technique is the Surfer leak test (<http://www.firewallleak tester.com/leak test15.htm>). ZABypass is another example of a leak test that uses this method.

With Outpost Security Suite Pro, every attempt to use DDE intercommunication is monitored with no exclusion, whether the process is open or not. The DDE inter-process communication control enables Outpost Security Suite Pro to govern the methods used by applications to gain command over legitimate processes. It prevents malware from hijacking a legitimate program and checks whether such DDE-level interactivity is allowed to be performed on network-enabled applications. In case such an attempt is detected, it triggers a legitimacy verification prompt.

Application window control

Windows allows applications to exchange window messages between processes. Malicious processes can gain control over other network-enabled applications by sending them window messages and imitating user input from the keyboard and/or mouse clicks. An example of using this technique is the Breakout leak test (<http://www.firewallleak tester.com/leak test16.htm>).

The crucial point here is program interactivity through the SendMessage, PostMessage API, and so on. This technique is used for legitimate inter-process interactivity, but can very easily be used for nefarious purposes by malicious individuals.

Outpost Security Suite Pro controls such attempts.

DNS query submission

The DNS Client service contains a vulnerability called DNS tunneling. Malicious code can transfer and receive any information using correct DNS packets to a correctly configured operating DNS server. An example of using this technique is the DNSTester leak test (<http://www.klake.org/~jt/dnshell/>).

Outpost Security Suite Pro performs double verification of any access to a DNS Client service, thereby providing a more secure system. This controls access to a DNS API even with the DNS Client service on, and thus benefits users who, out of compatibility concerns, cannot disable this service themselves. This functionality allows the assignment of permissions to a specific process to use the DNS Client service.

Network-enabled application launch

Malicious processes can launch your default web browser with command-line parameters (for example, with a pre-configured web address) in a hidden window, making the firewall believe a legitimate action is taking place. Firewalls that explicitly trust an application without looking beyond it to who actually launched it in the first place and what additional connection parameters are supplied, are unable to challenge the technique, and thereby allow confidential data to be transmitted from the computer. Examples of this technique are used by the Tooleaky, Ghost and Wallbreaker leak tests (http://www.firewallleaktester.com/leak_test2.htm, http://www.firewallleaktester.com/leak_test13.htm, http://www.firewallleaktester.com/leak_test11.htm).

Outpost Security Suite Pro watches every program started on a computer and controls who has permission to start each program with command line parameters protecting your browser against tampering. Beyond browsers, command-line launch control applies to all network-enabled applications, which are present in the configuration. Outpost Security Suite Pro will prompt the user as to whether such activity should be permitted for a particular program.

OLE application control

A relatively new technique has surfaced that controls application activity through OLE (Object Linking and Embedding) - a Windows mechanism, which allows one program to manage the behavior of another program on the computer. It uses the technique of OLE intercommunication to exchange data and commands between applications, for example, to manage the activity of Internet Explorer so it can send user-specific data to a remote location. An example of using this technique is the PCFlank leak test (http://www.pcflank.com/PCFlankleak_test.exe).

Outpost Security Suite Pro detects an OLE communication and asks the user if it is normal for that application to control other applications' activity.

Process memory modification

Several Trojan horses and viruses use sophisticated techniques that let them alter the code of trusted applications running in memory and thereby bypass the system security perimeter in order to perform their malicious activities. This is known as code injection or copycat vulnerability. Examples of using this technique are the Thermite and Copycat leak tests (http://www.firewallleaktester.com/leak_test8.htm, http://www.firewallleaktester.com/leak_test9.htm).

Outpost Security Suite Pro enables you to control the functions that can be used to write malicious code into a trusted application's address space and so prevent a rogue process from injecting their code into those processes. The entire memory space used by any active application on a computer is monitored by Outpost Security Suite Pro (not just that of a network-enabled application). If malware tries to modify a legitimate application's memory, Outpost Security Suite Pro detects it and displays a pop-up alert. The system works proactively: it allows you to permit or deny the modification of memory of other processes

at the application level. For example, Visual Studio 2005 would be able to modify memory, while the "copycat.exe" leak test would be disallowed from doing so. This feature protects against even unknown malware not yet detected by antivirus and anti-spyware vendors that exploits this vulnerability.

Low-level network access

Some network drivers allow direct access to the network adapter, which bypasses the standard TCP stack. These drivers can be used by sniffers and other malicious programs to get low-level network access. They pose an additional risk for the system as traffic passing through them cannot be screened by a firewall. The example of using this technique is MBtest leak test (http://www.firewallleaktester.com/leak_test10.htm).

Outpost Security Suite Pro allows the control of applications that request non-standard network access. This feature strengthens overall network security level by preventing outbound data leakage. The user is able to control an application's attempts to open a network-enabled driver; so without the user's authorization, an application is not able to send even the ARP or IPX data.

Driver load

Applications working under the superuser account can install kernel-mode drivers in order to get complete and unlimited access to the system and work on its behalf. This might be necessary to hide their presence within the system or disabling security systems. An example of using this technique are various kernel-mode rootkits.

Outpost Security Suite Pro controls attempts to install drivers and checks each driver file against its malware database before the driver is loaded into memory. If used carefully, this technique is 100% effective protection against rootkit installations on the system.

14.3 Using Macro Addresses

Outpost Security Suite Pro allows you to specify macro addresses in rule descriptions to facilitate the creation of rules. Instead of having to type IP addresses manually while creating rules for your Intranet communications or some Windows-based services (for example, DNS), you can use suggested macro definitions, to designate local networks as LOCAL_NETWORK, all DNS servers as DNS_SERVERS, etc.

Outpost Security Suite Pro automatically recognizes current macro values so you do not need to change host and subnet addresses whenever network adapter settings are changed. For example, a mobile user's protection will always be active since the rules on his laptop work regardless of what network he is connected to.

When you specify a local or remote address, you can select one of the following macros:

DNS_SERVERS

Specifies addresses of all DNS servers in your network.

LOCAL_NETWORK

Specifies addresses of all your local networks and addresses from the broadcast ranges available on your computer.

WINS_SERVERS

Specifies addresses of all WINS servers on your network.

GATEWAYS

Specifies addresses of all gateway servers for your network.

MY_COMPUTER

Specifies all IP addresses your computer has in different networks, including loopback addresses.

ALL_COMPUTER_ADDRESSES

Specifies all IP addresses your computer has in different networks, including broadcast and multicast addresses.

BROADCAST_ADDRESSES

Specifies addresses within broadcast ranges available to your computer. A broadcast address is an IP address that allows information to be sent simultaneously to all machines on a given subnet.

MULTICAST_ADDRESSES

Specifies addresses in multicast ranges. A multicast address is a single address that refers to multiple network devices. "Multicast address" is synonymous with "group address".

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