



OUTPOSTPRO

ANTIVIRUS

User Guide

Abstract

This is the complete and detailed reference to the Outpost Antivirus Pro 2009 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 Antivirus Pro may have other options and dialogs than the current version.

Table of contents

1 Welcome to Outpost Antivirus Pro!	4
1.1 System Requirements.....	4
1.2 Installing Outpost Antivirus Pro	5
1.3 Registering Outpost Antivirus Pro	10
2 User Interface and Controls Basics	12
2.1 The Toolbar	12
2.2 Left and Information Panels	13
2.3 System Tray Icon	14
2.4 Interface Language	16
3 Basic Configuration	17
3.1 Starting and Stopping Protection	17
3.2 Managing Protection Status.....	19
3.3 Creating a New Configuration.....	20
3.4 Running in Auto-Learn Mode.....	21
3.5 Protecting Configuration with a Password	22
3.6 Smart Advisor	23
4 Updating Outpost Antivirus Pro	24
4.1 Configuring Updates.....	24
4.2 Agnitum ImproveNet	25
5 Protecting a Host from Malicious Process Activity	27
5.1 Setting Local Security Level.....	27
5.2 Controlling Penetration Techniques	28
5.3 Controlling Application Components	29
5.4 Controlling Critical System Objects.....	31
5.5 Monitoring Process Activity.....	32
6 Protecting against Malware	33
6.1 Performing a System Scan	33
6.1.1 Selecting Scan Type	33
6.1.2 Selecting Objects to Scan	34
6.1.3 Scanning Specified Locations	35
6.1.4 Removing Detected Malware.....	36
6.1.5 Viewing Scan Results.....	37
6.2 Real-Time Protection	38
6.3 Scanning Mail Attachments	39
6.4 Malware Quarantine	40
6.5 Scheduling System Scan	41
7 Controlling Online Activities	42
7.1 Site Blacklist	42
7.2 Blocking Private Data Transfers	42
8 Protecting Internal Components	45
9 Uninstalling Outpost Antivirus Pro	46
10 Tracking system activity	47
10.1 Logging debugging information	47
11 Appendix	49
11.1 Troubleshooting	49
11.2 Understanding Penetration Techniques.....	49
11.3 Using Macro Addresses	51
About Agnitum	52

1 Welcome to Outpost Antivirus Pro!

New types of threats require new forms of protection. Having come to your computer via infected internet sites, with infected e-mail messages, flash-cards, mp3-players and cameras, modern malware damages your documents, Malware steals your identities, money, and other valuable electronic commodities.

To fully protect against these new risks, an effective antivirus solution must deploy a multi-layered approach, providing proactive defense along with protection from information leakage and blocking malware and phishing Internet sites. 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 antivirus product—Outpost Antivirus Pro. It is aimed at protecting your computer against viruses, Malware, and data leakage.

Key Benefits

- The product's lightweight yet effective malware scanner detects and quarantines or directly removes viruses, Malware 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.
- Host Protection monitors program behaviors and interactions in order to proactively defend against unauthorized activity. It also blocks Trojans, Malware, and all kinds of sophisticated hacking techniques that try to compromise your system's security or steal your data.
- Outpost Antivirus 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 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 Antivirus' interface, settings, and functionality. For more information about features and for additional documentation, please visit <http://www.agnitum.com/products/antivirus/>.

1.1 System Requirements

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

- CPU: 450 MHz Intel Pentium, AMD or compatible;
- Memory: 256 MB;
- Hard disk space: 50 MB.

Note:

- Outpost Antivirus 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.
- Outpost Antivirus Pro should not be run with any other security software. Running Outpost Antivirus Pro with other security products can result in system instability (i.e. crashes) and can cause your system to operate in an insecure mode.

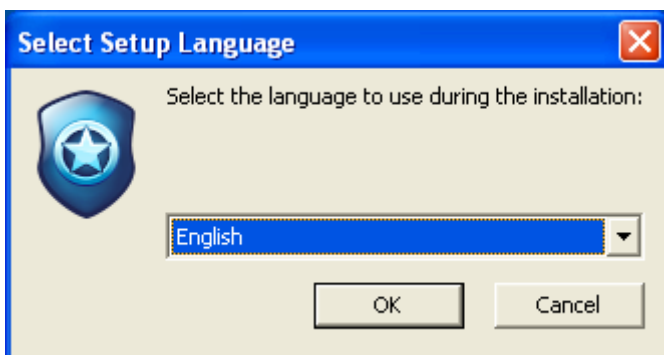
1.2 Installing Outpost Antivirus Pro

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

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

1. **Very Important!** Before installing Outpost Antivirus Pro, uninstall any other security software on your computer and reboot.
2. Close all open applications.
 - a) if you install the product downloaded from the site, click **OutpostAntivirusProInstall.exe**;
 - 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 (OutpostAntivirusProInstall.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\OutpostAntivirusProInstall.exe
3. Click the **OK** button.
4. 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.

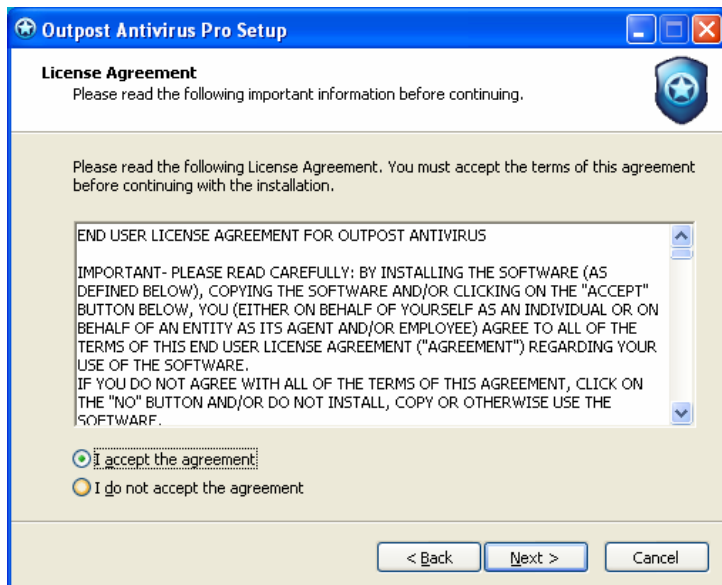


Choose the language for Outpost Antivirus Pro interface and click **OK**. Setup will display the **Welcome** dialog presenting basic features of the product:

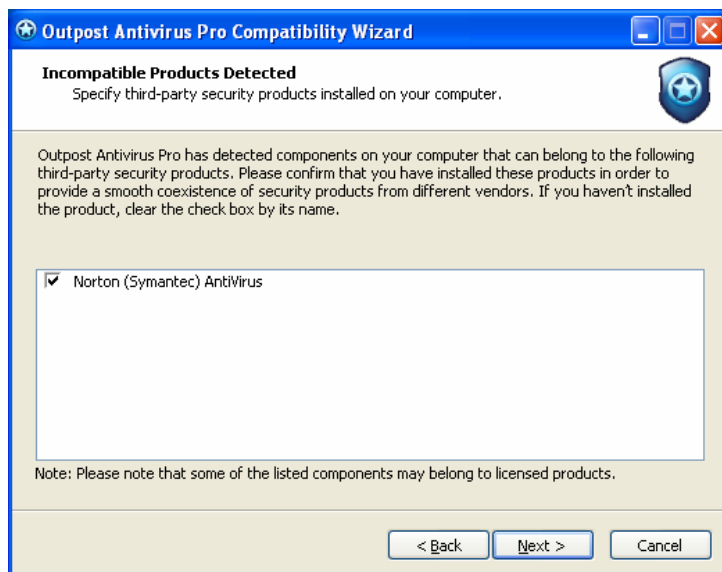


After clicking the **Next** button you will be asked to accept the License Agreement to use the **Outpost Antivirus Pro**.

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:



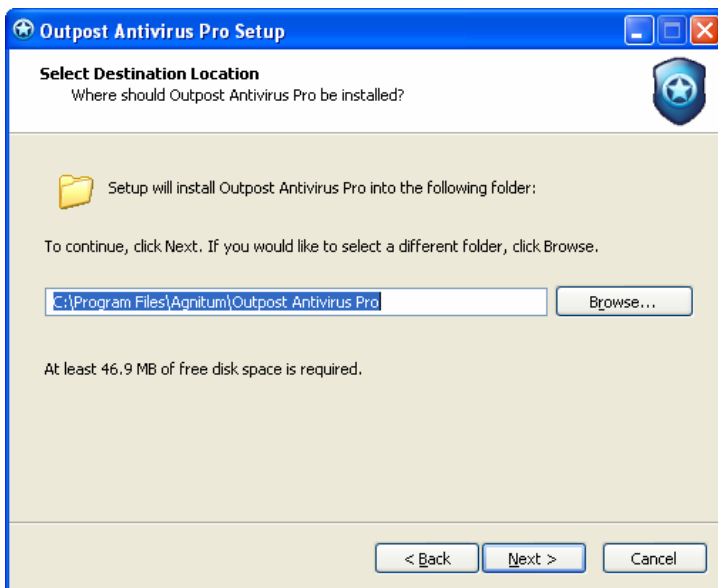
In case you have not removed any third-party security software, the setup wizard will display a prompt pointing at detecting incompatible software:



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

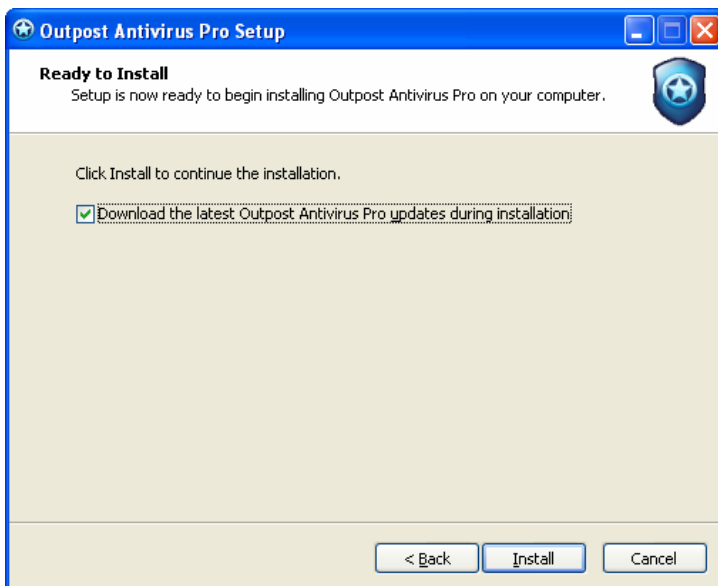
On detecting *a partly compatible product* the wizard will offer you one of the possible options to apply to the product.

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

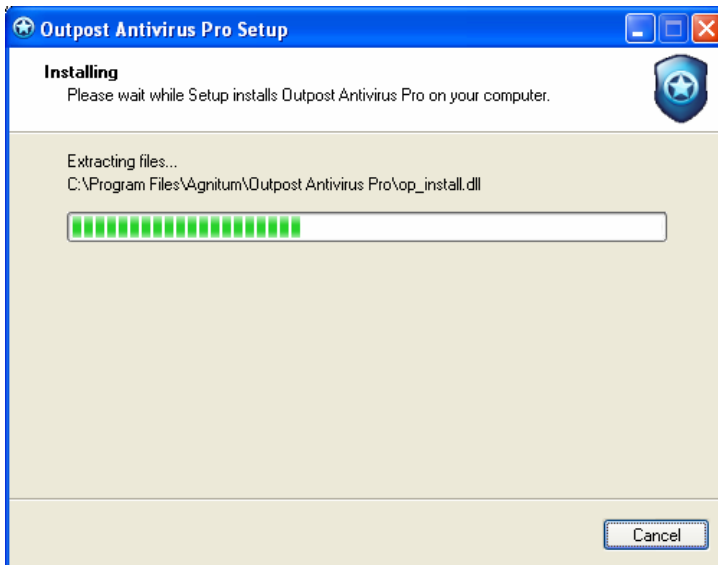
If you want to change the default file location, click **Browse**. Select the folder or create your own one and click **OK**. Click **Next** to proceed to the last step before actual installation:



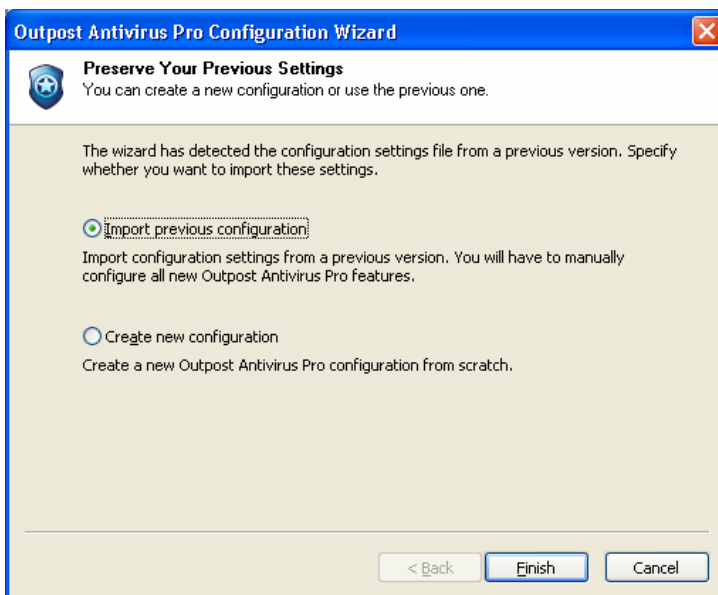
Select the **Download the latest Outpost Antivirus Pro updates during installation** option to download latest malware signatures' bases and settings for the product.

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:

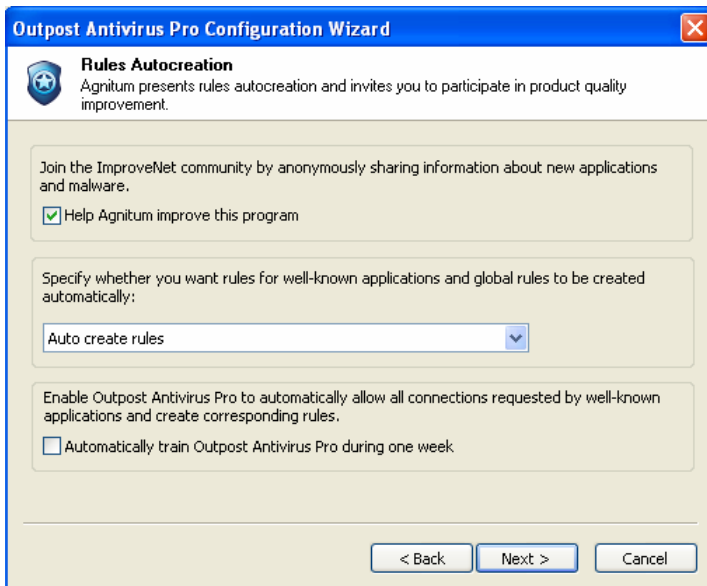


After the installation is finished, the **Configuration Wizard** will help you create a new configuration or import the previous if you install the product over an earlier version:



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 Antivirus Pro installation.

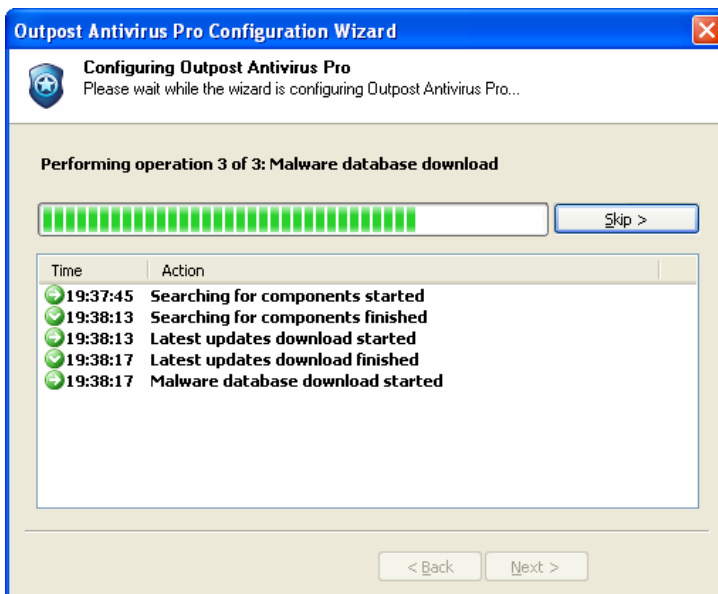
The **Rules Autocreation** step, which lets you to enable rules autocreation, so rules for well-known applications are created automatically when they first request an action (for example, process memory modification):



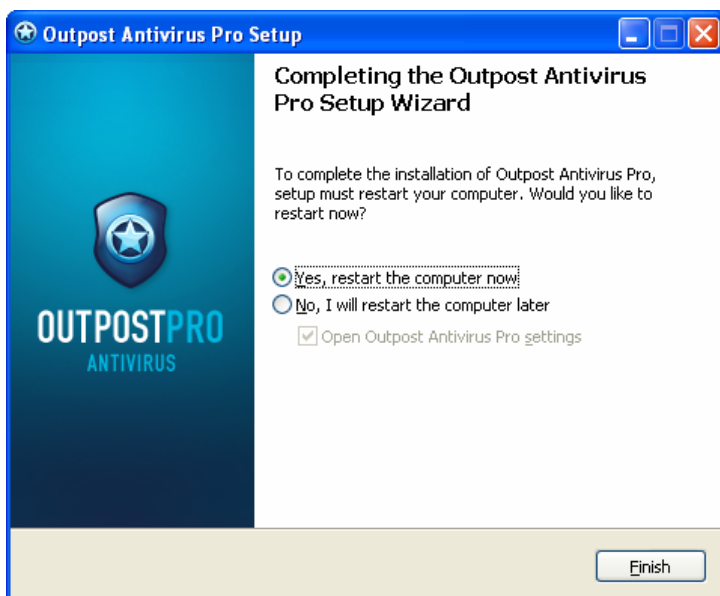
The **Automatically train Outpost Security Suite Pro during one week** option allows product to create necessary rules automatically.

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

After clicking **Next**, Outpost Antivirus Pro automatically scans your system and adjusts all its settings without your supervision. It configures necessary settings and builds the Component Control database:



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



Important:

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

1.3 Registering Outpost Antivirus Pro

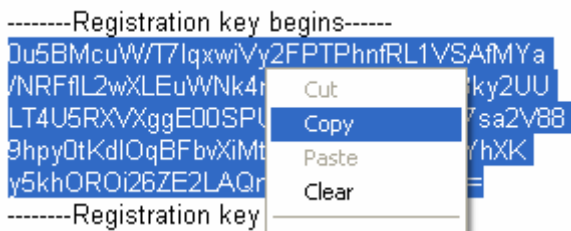
Outpost Antivirus Pro is available for your free evaluation. You are entitled to evaluate the software during the trial period with no obligation to pay. After the trial period, if you decide to keep the software and would like to receive free annual updates, you must register your copy with us for a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

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

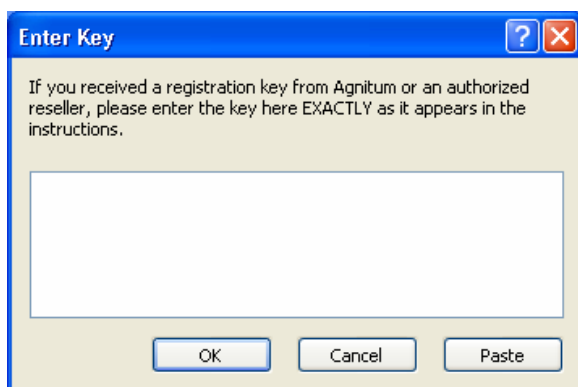
If you downloaded your copy from Agnitum's web site, to register your version, you need to purchase your registration key. Follow the instructions on the page <http://www.agnitum.com/purchase/antivirus/> and you will receive your registration key by e-mail.

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 Antivirus 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 Antivirus Pro license, you actually get two licenses:

- A license for Outpost Antivirus Pro usage (lifelong);
- A license for free upgrades and support for the period of your licensing term (including the latest Outpost Antivirus Pro versions).

After the licensing term is finished 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 Antivirus Pro. To purchase a renewal, visit this page:

<http://www.agnitum.com/purchase/renewal/index.php>.

Note:

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

2 User Interface and Controls Basics

When you launch Outpost Antivirus Pro for the first time, its main window is displayed. The main window is your central control panel for the product. 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 Antivirus 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 Antivirus's [system tray icon](#).
2. Select **Show/Hide**.

To close the Outpost Antivirus 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 product 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 Antivirus Pro's current state.

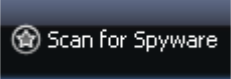
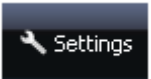

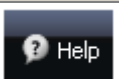
2.1 The Toolbar

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:



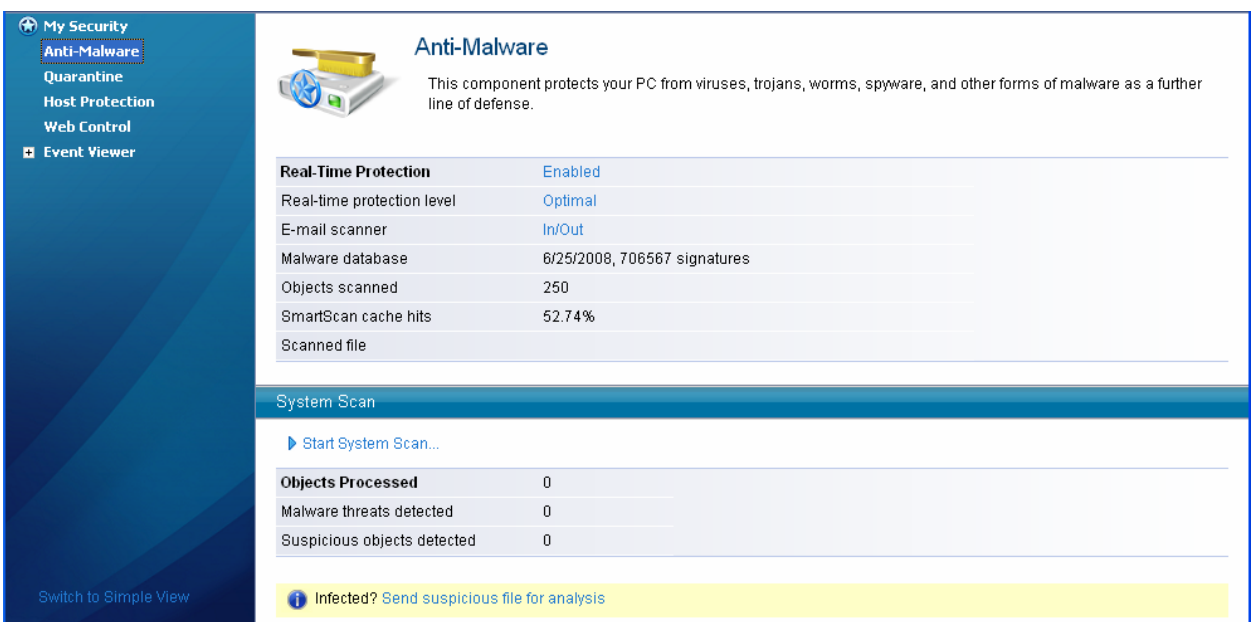
These are the buttons found on the toolbar:

Button	Function
	Starts the malware system scan .
	Opens Outpost Antivirus Pro's Settings dialog.
	Downloads the latest product updates including anti-malware databases.
	Opens the context help file.

2.2 Left and Information Panels

To display information so you can easily find it, Outpost Antivirus 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:



The screenshot shows the 'Anti-Malware' information panel. On the left is a navigation menu with options: My Security, Anti-Malware (selected), Quarantine, Host Protection, Web Control, and Event Viewer. The main panel displays the following information:

- Anti-Malware**: This component protects your PC from viruses, trojans, worms, spyware, and other forms of malware as a further line of defense.
- Real-Time Protection**: Enabled
- Real-time protection level: Optimal
- E-mail scanner: In/Out
- Malware database: 6/25/2008, 706567 signatures
- Objects scanned: 250
- SmartScan cache hits: 52.74%
- Scanned file: (empty)

Below this is a 'System Scan' section with a 'Start System Scan...' button and a table of scan results:

Objects Processed	0
Malware threats detected	0
Suspicious objects detected	0

At the bottom, there is a yellow banner with the text: 'Infected? Send suspicious file for analysis'.

For your convenience, Outpost Antivirus Pro allows switching between simple and expert views of the main window depending on your needs and abilities to manage security products. By default, the product will display its **Simple View**. If you are not an advanced user, it would be easier for you to use the **Simple View** of the screen, as it does not contain any pages that might be difficult to understand. If you are an advanced user, we recommend switching to **Expert View**, which will provide you with more

information about the product's operation and system performance. That could be useful for tracking system activity and taking steps if anything happens.

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

Note:

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

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

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

- **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.

- **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.

- **Web Control**

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

- **Event Viewer**

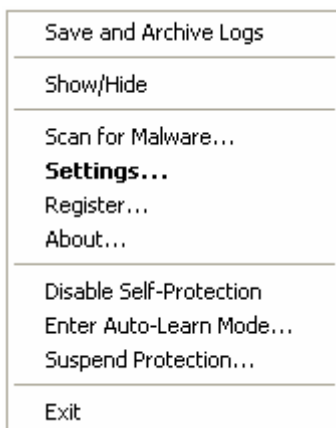
Displays detailed statistics for all past system and product activities by category.

2.3 System Tray Icon

By default, Outpost Antivirus Pro is automatically loaded when Windows starts up to provide immediate protection of your system at the earliest stage. Once it is loaded, the icon with the light-blue star in the dark-blue ring (Outpost Antivirus 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 Antivirus 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 the system tray icon you get its context menu.

The system tray icon menu looks like the following:



The following commands are available on this menu:

- **Save and Archive Logs**

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

- **Show/Hide**

Displays or hides Outpost Antivirus 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 Antivirus Pro updates and support.

- **About**

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

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

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

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

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

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

Disables (enables) Outpost Antivirus Pro [protection](#).

- **Exit**

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

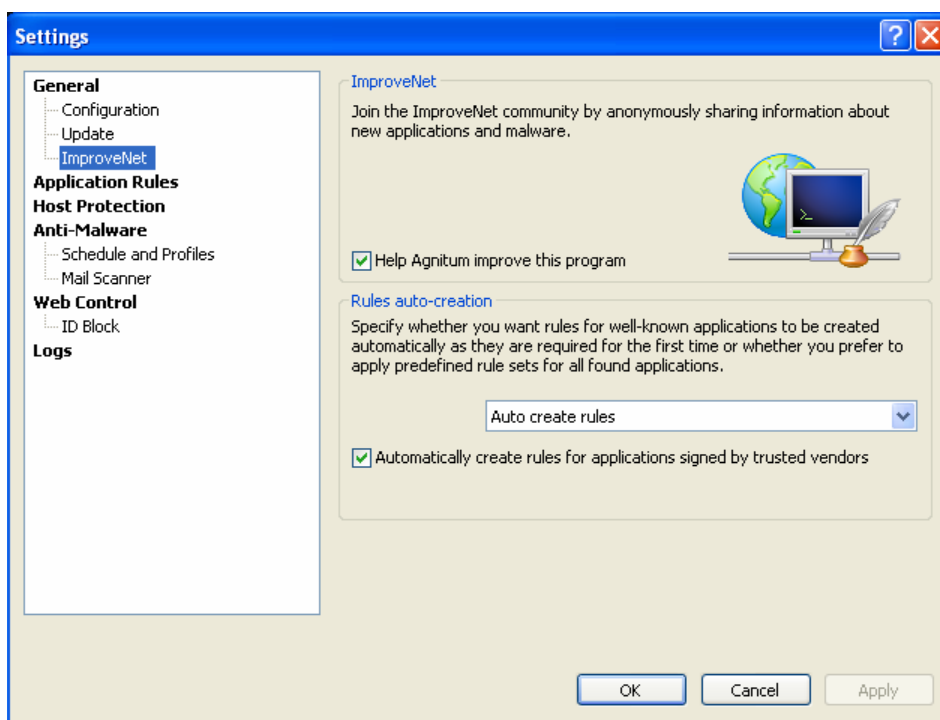
Note:

- The system tray icon is not visible while Outpost Antivirus Pro runs in [background mode](#).

2.4 Interface Language

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

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




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

3 Basic Configuration

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

This section gives a brief overview of Outpost Antivirus 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](#) and how to [protect your settings](#) from unauthorized alteration.

3.1 Starting and Stopping Protection

By default, Outpost Antivirus 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 light-blue star in the dark-blue ring  is displayed in the system tray, the right end of the Windows task bar. When you see this icon, it means that Outpost Antivirus Pro is operating and protecting you.

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

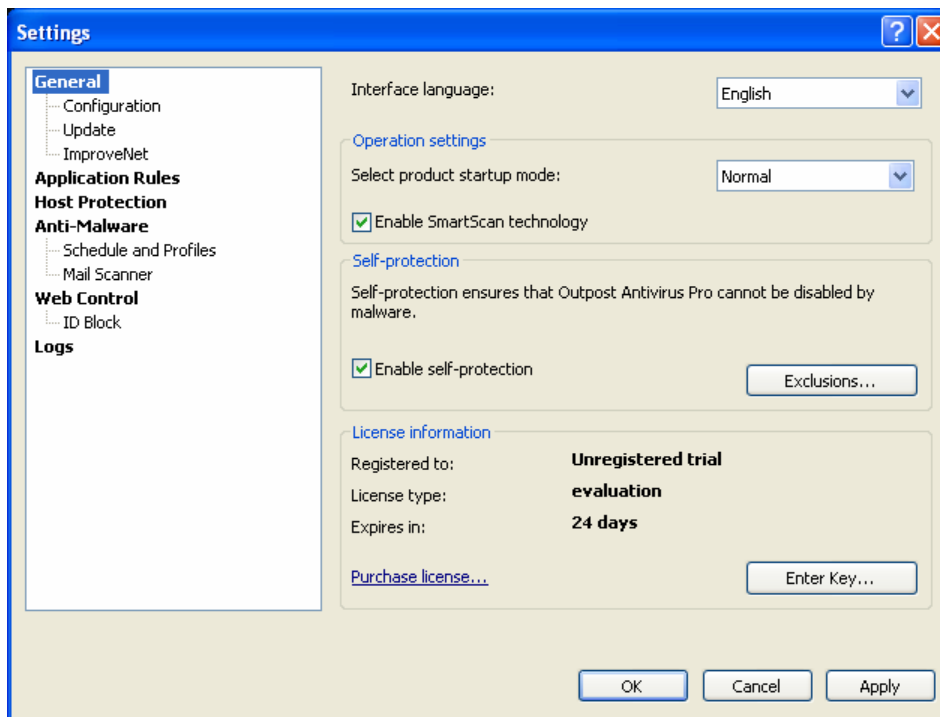
To completely stop Outpost Antivirus Pro so it no longer protects your system, right-click the product's icon in the system tray, click **Exit**, select **Exit Outpost Antivirus Pro and shutdown service** from the list and click **OK**.

Startup mode

Outpost Antivirus 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 Antivirus Pro automatically when you turn on your computer and displays its icon in the system tray.
- **Background** - when in background startup mode, Outpost Antivirus Pro runs invisibly without displaying its system tray icon or any of its dialog windows. This makes the product invisible to users.

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



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

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

Suspending protection

Outpost Antivirus 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 product's icon in the system tray and click **Suspend Protection**. You will be asked for the duration you'd like the product 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 product's icon and selecting **Resume Protection**.

Disabling Outpost Antivirus Pro's components

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






- 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 **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 **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 Antivirus 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 Managing Protection Status

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

Component	Status	
Self-protection	Enabled	
Host protection level	Optimal	
Real-time malware protection	Enabled	
Malware database	6/23/2008	
License	Trial, 30 days left Purchase...	

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

- **Self-protection mode.** Clicking the link in the **Status** column will change the self-protection status. See [Protecting Internal Components](#) for details.
- **Host protection level.** Clicking the link in the **Status** column will open the **Host Protection** settings, allowing you to change this level. See [Setting Local Security Level](#) for details.
- **Real-time malware protection status.** Clicking the link in the **Status** column will open the Anti-Malware settings, allowing you to change them. See [Real-Time Protection](#) for details.
- **Malware database date.** Clicking the **Update** link available in the case of an outdated database will start the update process. See [Updating Outpost Security Suite Pro](#) for details.
- **License information.** Displays the type of license you have and if you are not registered yet, allows you to easily register the product by clicking the **Register** link. See [Registering Outpost Security Suite Pro](#) for details.

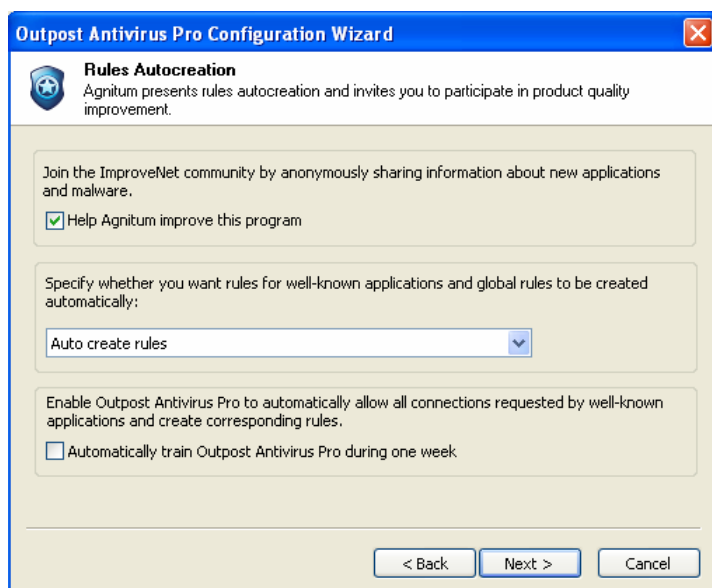
If a component operates in a mode, which is different from the optimum (recommended), the corresponding line will be highlighted yellow to let you know that this component does not provide the required level of protection. If the component is disabled, the corresponding line will be highlighted red to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

3.3 Creating a New Configuration

The exact state of Outpost Antivirus Pro at any moment of time is represented by all of its settings, which include: components security levels and host protection level, 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. 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**.

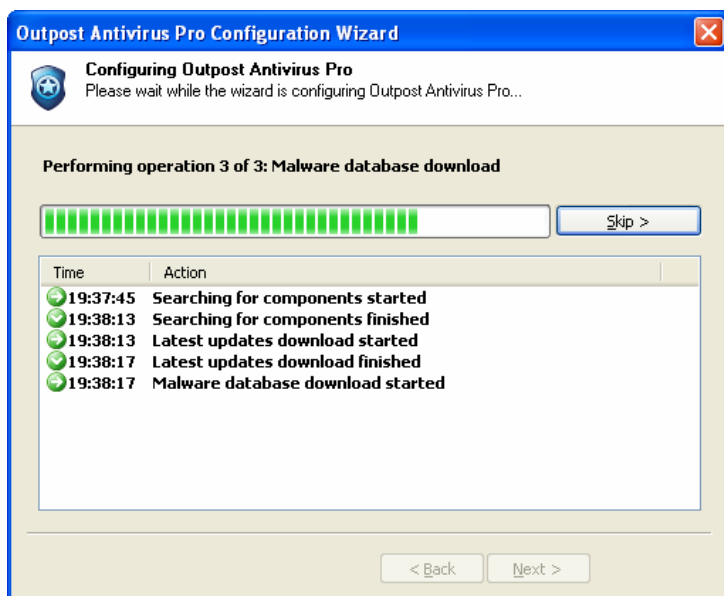
The **Rules Autocreation** step, which lets you to enable rules autocreation, so rules for well-known applications are created automatically when they first request an action (for example, process memory modification):



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 Antivirus Pro, select the **Help Agnitum improve this program** option.

After clicking **Next**, Outpost Antivirus Pro automatically scans your system and adjusts all its settings without your supervision. It configures necessary settings and builds the Component Control database:



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 Antivirus 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 Antivirus Pro, the configuration file that is currently in use is saved so it will be automatically loaded the next time Outpost Antivirus Pro is started.

3.4 Running in Auto-Learn Mode

To reduce the number of prompts during the initial stage of Outpost Antivirus 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 Antivirus Pro assumes all new program activity is legitimate and consequently allows process interaction to all requesting programs. As different programs interact with other software for the first time, Outpost Antivirus Pro memorizes their identities and creates allowing rules for all the requested actions. 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 process, it is managed according to these created rules.

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

After the specified period, the software automatically enables the created rules and downloaded updates.

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

Note:

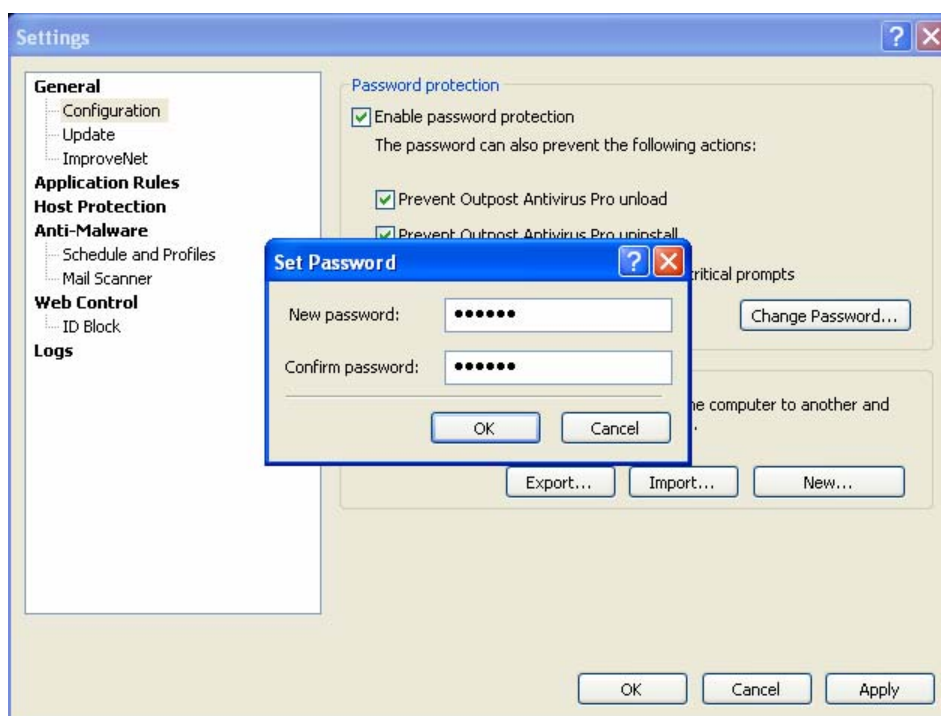
- Auto-Learn Mode can pose a security risk because allowing rules are created for every requested action. So while in Auto-Learn mode, be sure you are not running any unknown or untrusted applications and not visiting objectionable sites.

3.5 Protecting Configuration with a Password

Outpost Antivirus 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.

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 Antivirus 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 Antivirus settings will be available to every person who uses the computer.

You can additionally protect Outpost Antivirus 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.

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

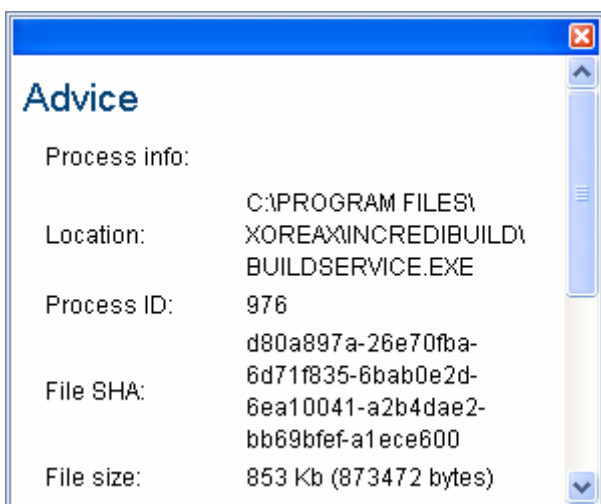
Note:

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

3.6 Smart Advisor

During its operation, Outpost Antivirus 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 action has no rule and user response is needed.

To assist the user in making a decision, Outpost Antivirus Pro provides additional information on the subject and suggestions which are available via the **Smart Advisor** link included in the prompt dialog. After clicking the **Smart Advisor**, a new window provides details for selecting Outpost Antivirus 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:



4 Updating Outpost Antivirus 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 Malware 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 Antivirus 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 Antivirus 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 Antivirus Pro Update wizard will perform all the necessary tasks, downloading the latest available product components 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 Antivirus Pro > Update**.

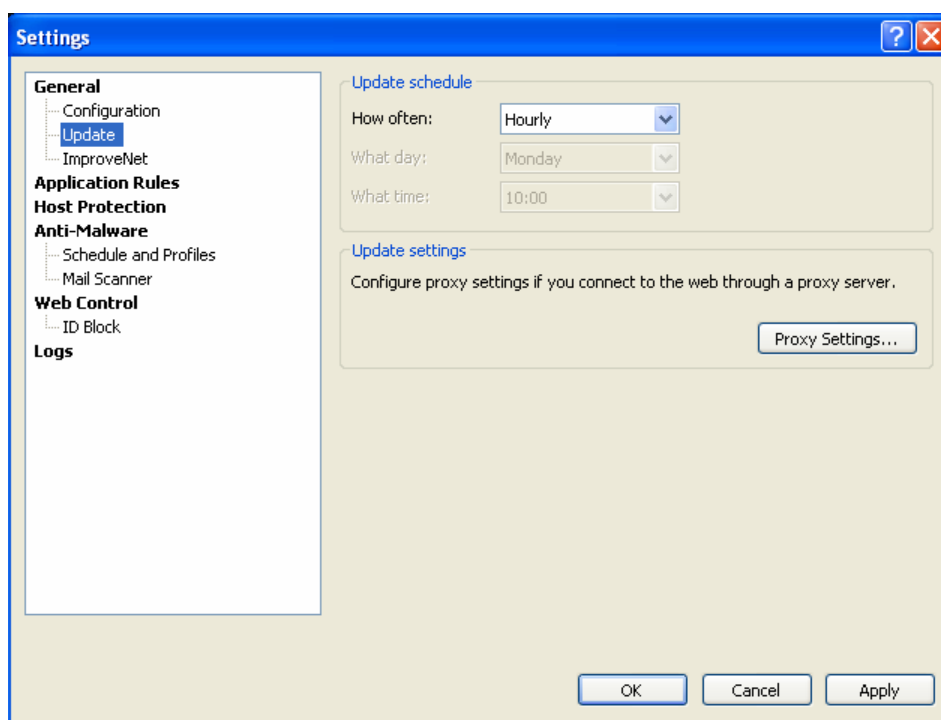
Agnitum lets you change the regular [updates schedule](#) and suggests that you personally may want to help in updating Outpost Antivirus Pro's rules by participating in a completely free [Agnitum ImproveNet](#) program.

Note:

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

4.1 Configuring Updates

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

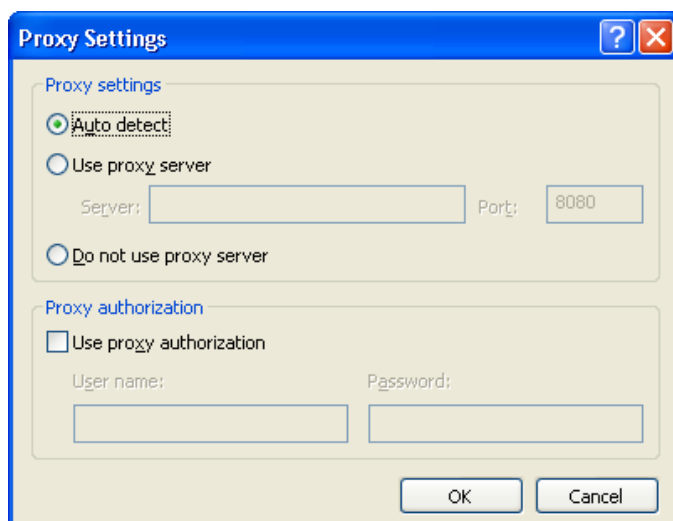


By default, updates take place on an hourly basis, however, you can choose a time when Outpost Antivirus Pro downloads updates on your own. To do this, click the **Settings** button on the toolbar and select the **Update** page.

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.

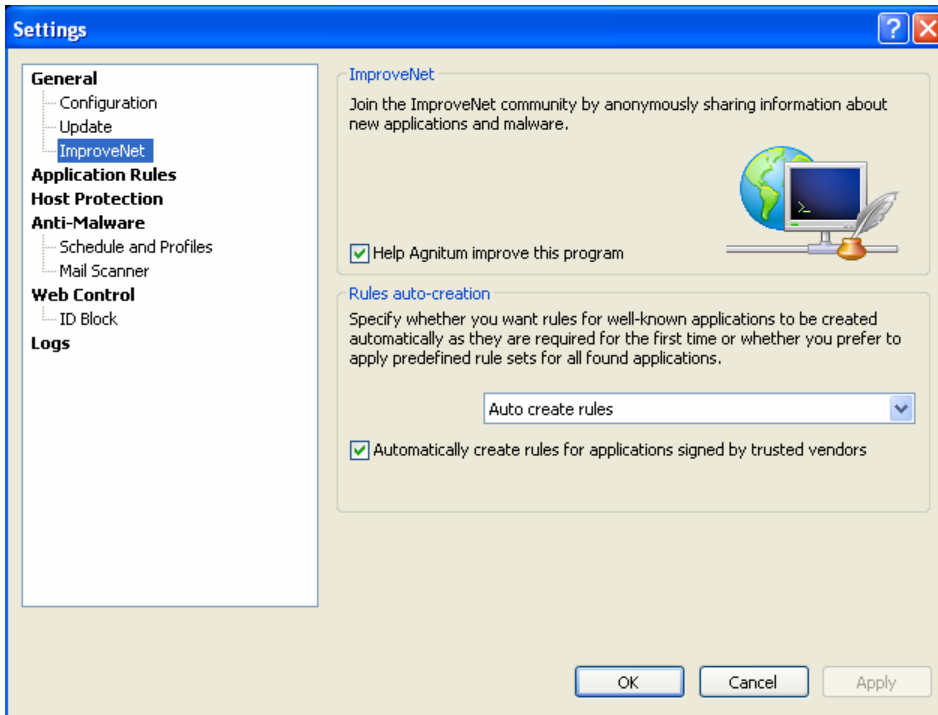
4.2 Agnitum ImproveNet

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 Antivirus Pro's database of known applications, so that many more rules are available to you. This will reduce the number of dialog pop-ups that require your attention.

With your consent, Outpost Antivirus 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 Antivirus Pro simply collects data on the 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.

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:

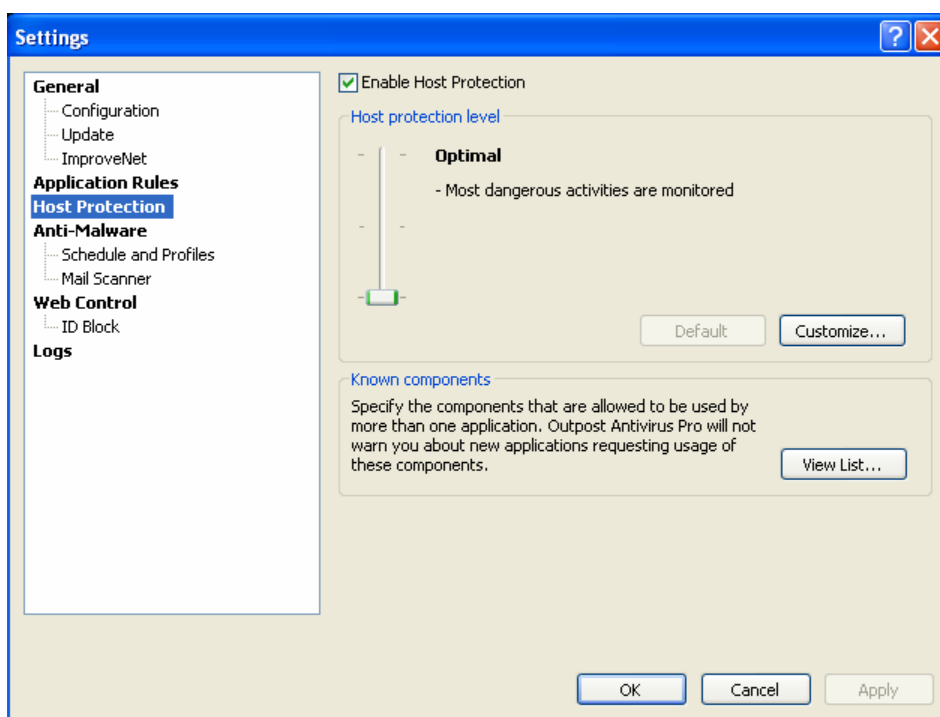


5 Protecting a Host from Malicious Process Activity

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 Antivirus Pro's Host Protection does not allow such program activity and thus fully protects you from Trojans, Malware 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 Antivirus Pro. Turning Host Protection off severely reduces your system's security level, as it is no longer having each system activity monitored.

5.1 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. 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.

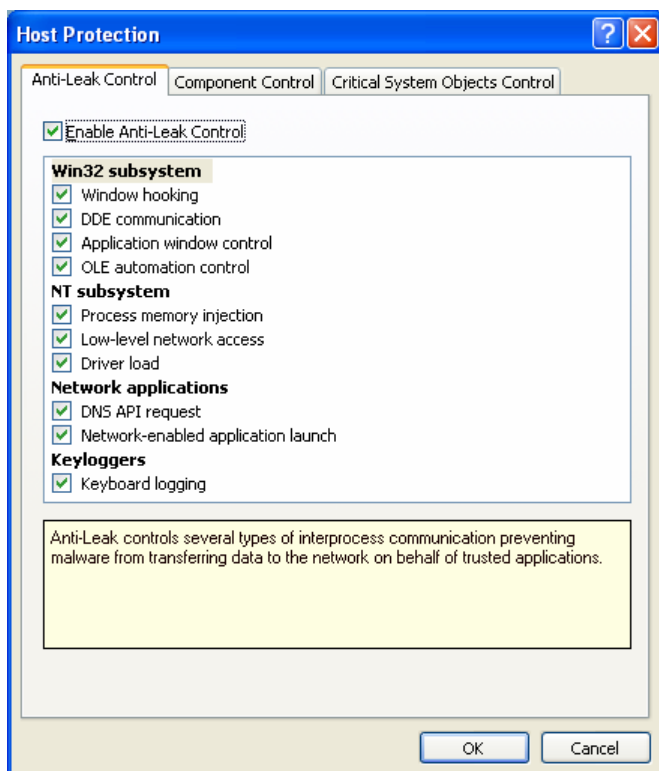
To customize your security level to better suit your needs, click **Customize**. In the appeared dialog box you can set parameters for [Anti-Leak Control](#), [Component Control](#) and [Critical System Objects Control](#) according to your specific requirements.

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

5.2 Controlling Penetration Techniques

There are several advanced penetration schemes that allow malicious software to bypass the security perimeter of a PC. Outpost Antivirus 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 Malware 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. All the techniques are divided into groups according to their types and possible actions within the system. The available settings allow you to select whether a technique should be controlled by Outpost Antivirus Pro or not. If you want the product to control a technique, select the check box next to it.



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), open the **Application Rules** page and double-click the required application. On the **Anti-Leak Control** tab of the **Modify Rules** dialog box, you will be able to change the application activities by clicking the key word in the **Action** column and selecting the desired action. The following actions are possible:

- **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.
- **Use Global.** Global settings will be inherited for the selected activity.

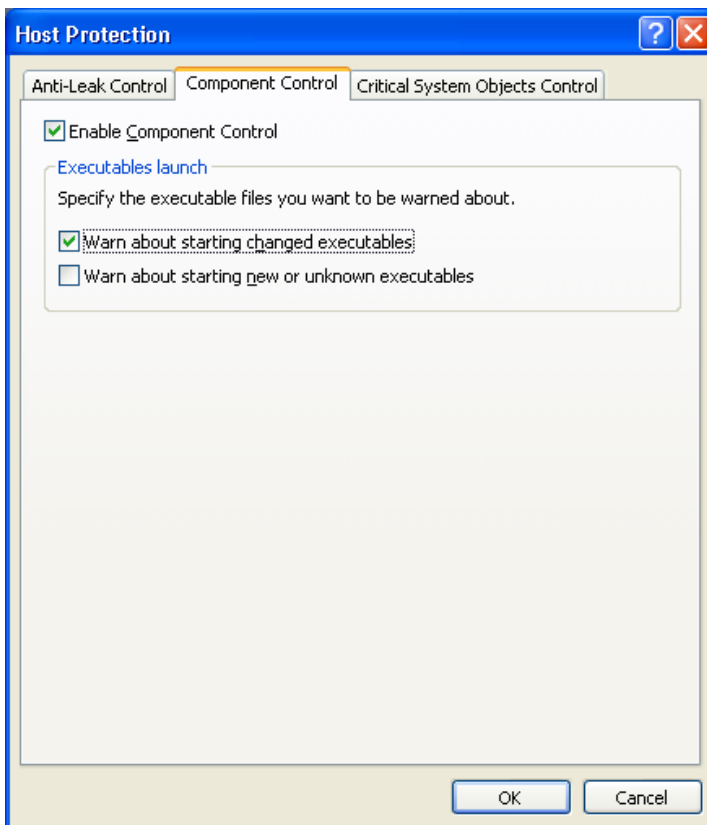
Note:

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

5.3 Controlling Application Components

Applications typically have dozens of modules, any of which can easily be substituted by a Trojan made to execute a malicious code on your computer. Outpost Antivirus Pro monitors applications and if the executable of an application has been changed and the application is about to establish a connection, Outpost Antivirus Pro will inform you of the changed executable 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.

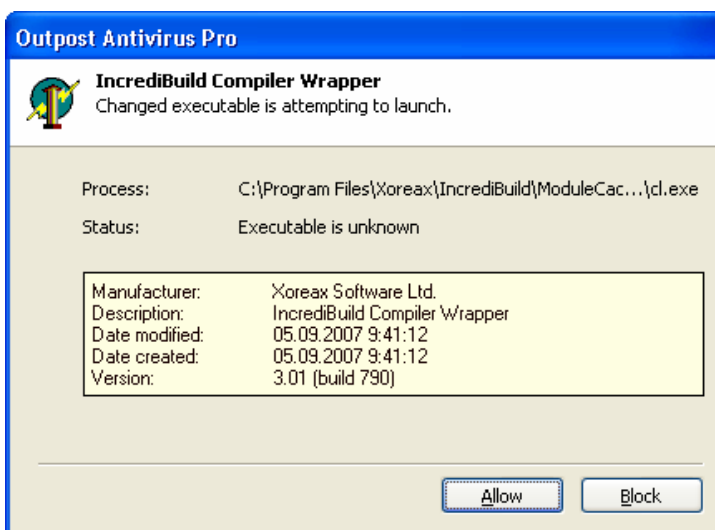
To change the Component Control settings, click **Settings > Host Protection > Customize** and select the **Component Control** tab. To enable/disable Component Control, select/clear the **Enable Component Control** check box:



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

Each time a monitored event occurs, Outpost Antivirus 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:



Tip:

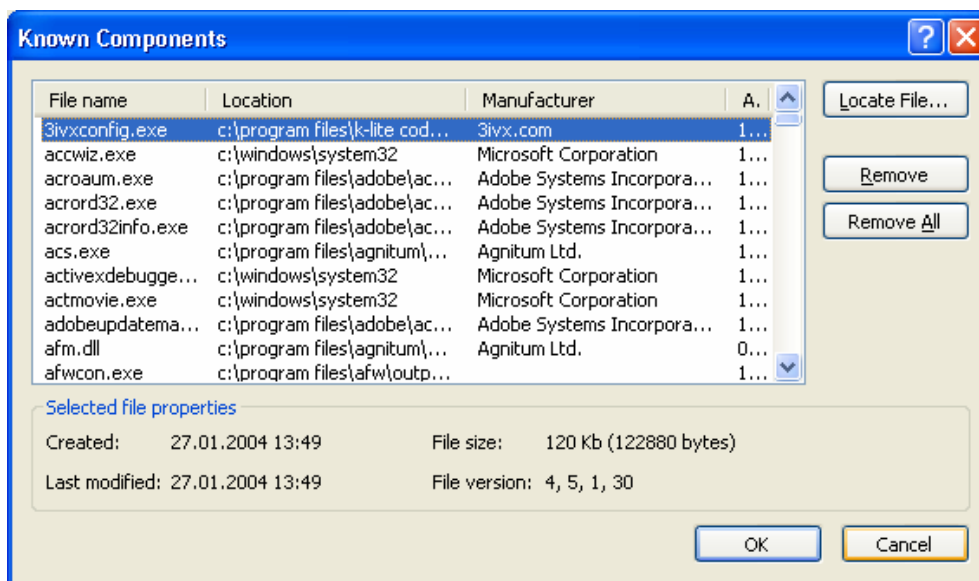
- To improve check performance, you can have Outpost Antivirus Pro create check status cache files in each folder by selecting the **Enable SmartScan technology** check box on the **General**

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 Antivirus 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.

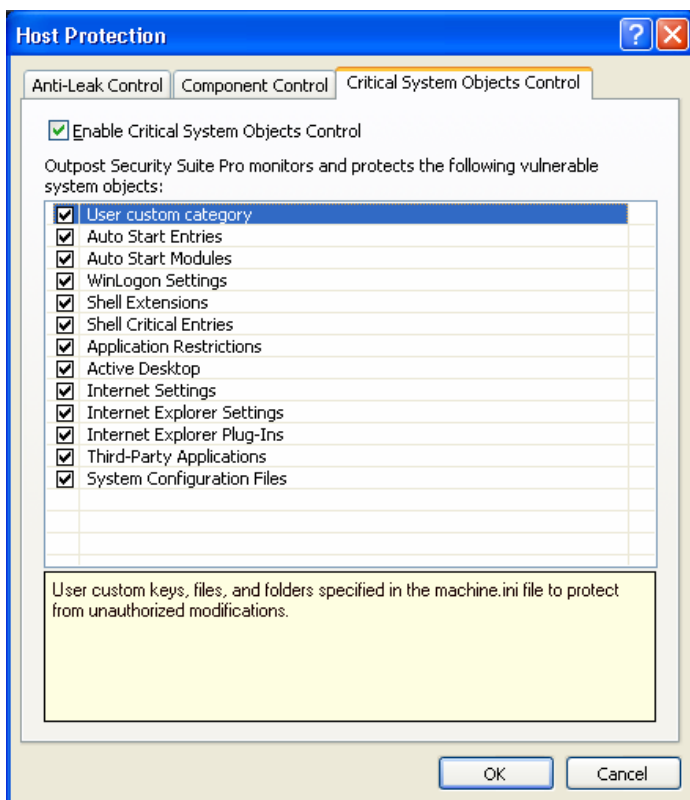
5.4 Controlling Critical System Objects

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 Antivirus 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 Antivirus Pro, clear its check box. You will always be able to restore the default settings at any time.

5.5 Monitoring Process Activity

To view the list of processes currently running on the system, select **Process Activity** in the main product window. By default, child processes are grouped under their parent process's name.

Use the **Toggle Sort** command on the process's shortcut menu to switch to "flat" mode where you can sort displayed data by values in any column by clicking the corresponding column name. To return to the default view, right-click anywhere inside the information panel and click **Toggle Sort** once more.

You can change not only the view of the panel, but also the content and number of the columns displayed by right-clicking anywhere inside the information panel and selecting the **Columns** command. On the **Columns** tab select the columns you want to be displayed; you can select any or all of the columns. You can also change the order the columns are displayed by selecting the name of the column and using the **Move Up/Move Down** commands to position where you want the column shown.

The **Status** column indicates whether the process is signed by a trusted vendor or known via the ImproveNet system (**Verified**) or unknown for the product (**Unknown**).

Note:

- The Process Activity log is available only in **Expert View**.

6 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, 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. Anti-Malware capabilities are provided 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.

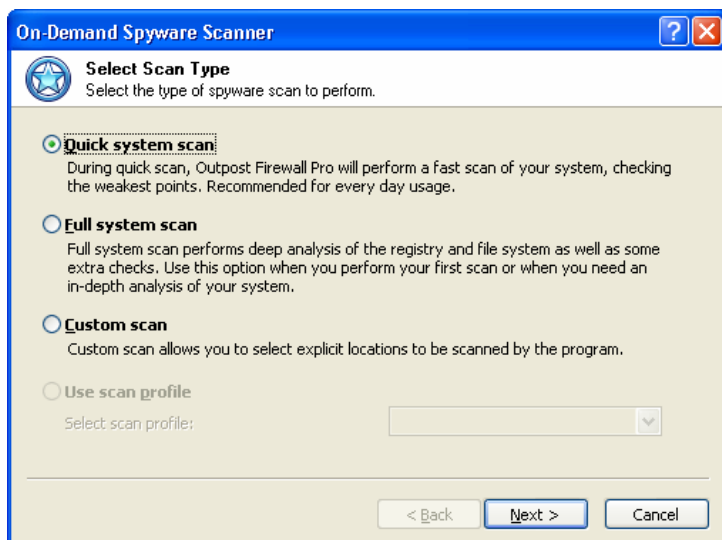
6.1 Performing a System Scan

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 Antivirus 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](#).

6.1.1 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 for 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 Antivirus 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.

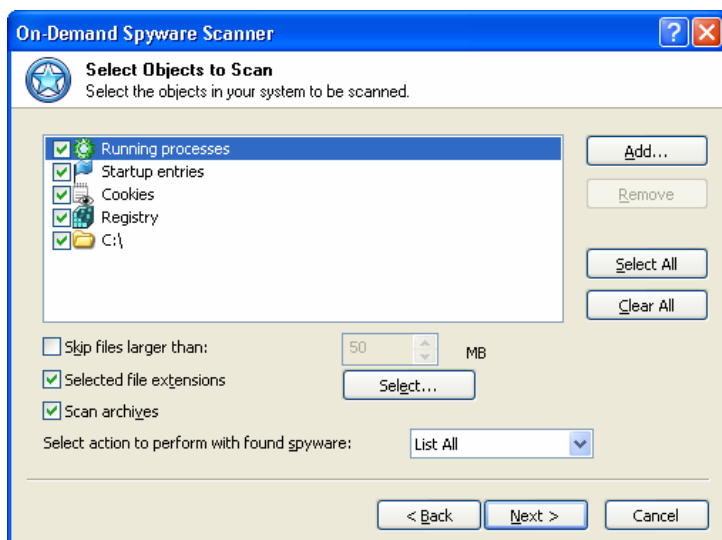
In the **Edit Scan Profile** window, you will be able to specify [the objects to be scanned and other scanning settings](#). After specifying the settings, click **OK** to save your profile and it will be displayed in the **Scan Profiles** list.

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.

6.1.2 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 Antivirus Pro will try to cure the suspicious object. If the object cannot be cured, Outpost Antivirus Pro will automatically quarantine it.
- **Quarantine.** Outpost Antivirus Pro will place the detected malware in [quarantine](#).
- **Remove.** Outpost Antivirus Pro will delete the detected malware once it is detected.

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

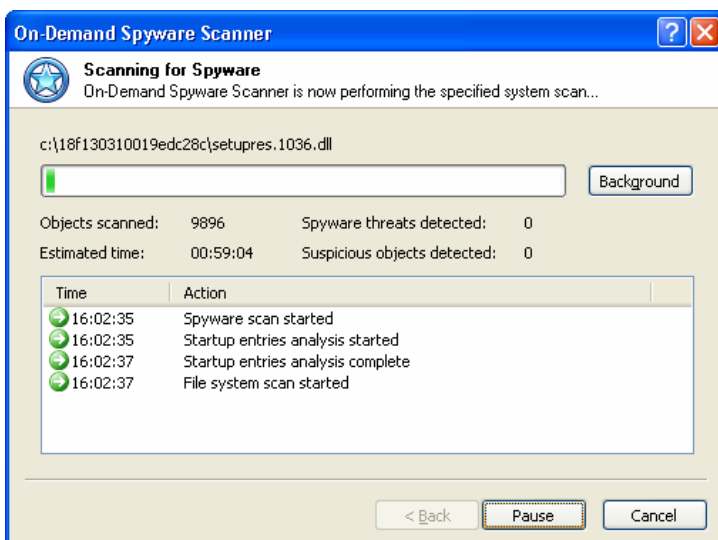
When you have specified the objects and locations to scan, click **Next** to start the [scan process](#).

Note:

- 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 Antivirus Pro scans files contained in ZIP, RAR, and CAB archives.

6.1.3 Scanning Specified Locations

After clicking **Next**, Outpost Antivirus 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:



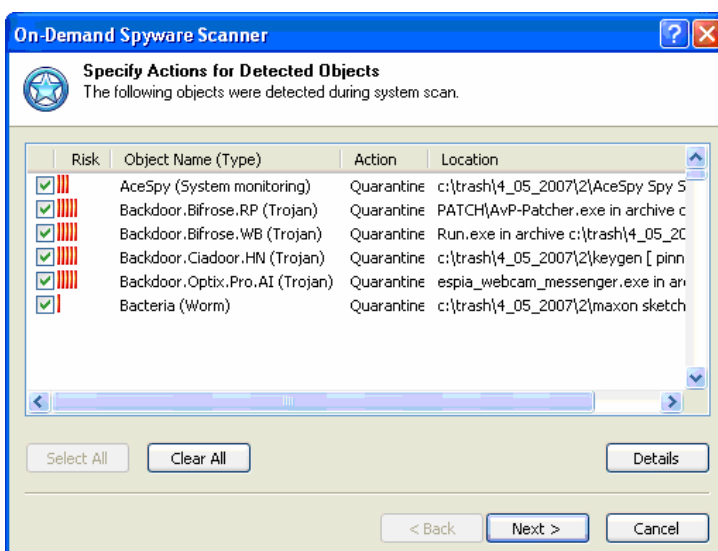
The scanning process can run in background mode. If you want to work with Outpost Antivirus Pro while the scan is underway, click the **Background** button and the wizard will be minimized. To see the full window again, select **Anti-Malware** on the left panel of the main window and click **Show Details**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

6.1.4 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 Antivirus 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 Antivirus Pro will ignore the programs on the exclusions list and will display no alerts when detecting their activity. Also, these programs will not be displayed on the list of detected spyware.

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

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

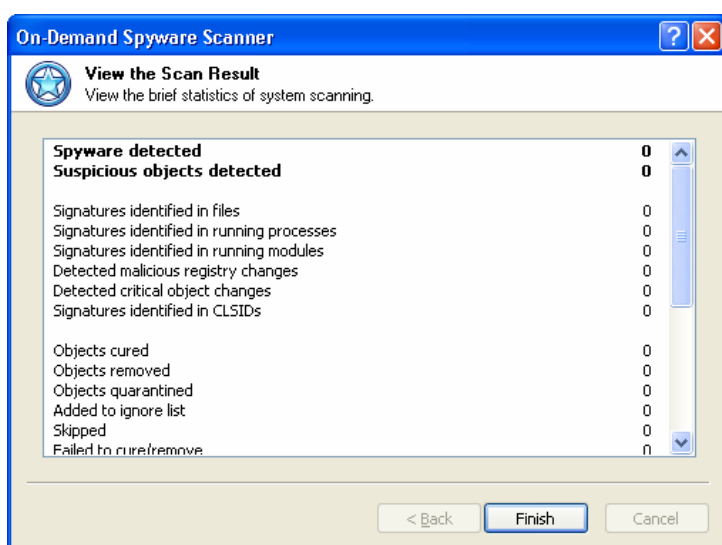
You can later remove items from the exclusions lists using the **Exclusions** button on the **Anti-Malware** dialog page of the product **Settings** window.

Important:

- A cookie is not malware, but it can be used as a holding file to transfer private information from your computer to a specific web site. Malware 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).

6.1.5 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:



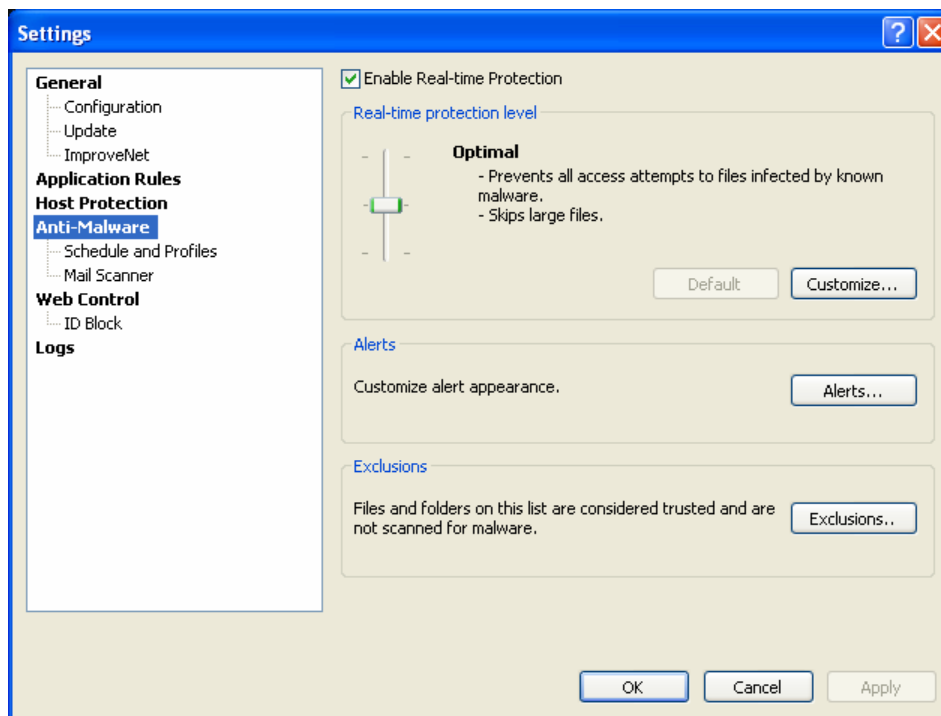
Note:

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

6.2 Real-Time Protection

The Anti-Malware component provides real-time non-stop protection against malware. 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:

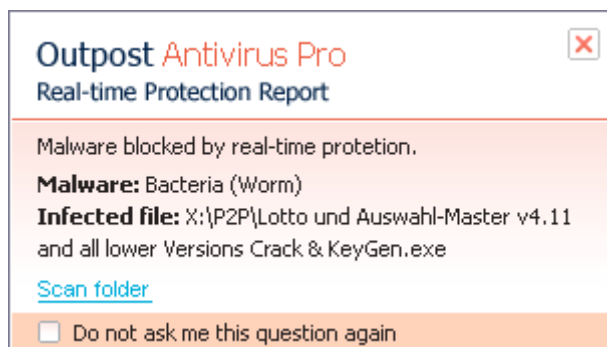


Tip:

- To improve scan performance, you can have Outpost Antivirus 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 Antivirus 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 Antivirus Pro will display a visual alert and play the specified sound file each time malware is detected and cured, quarantined or removed. 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.

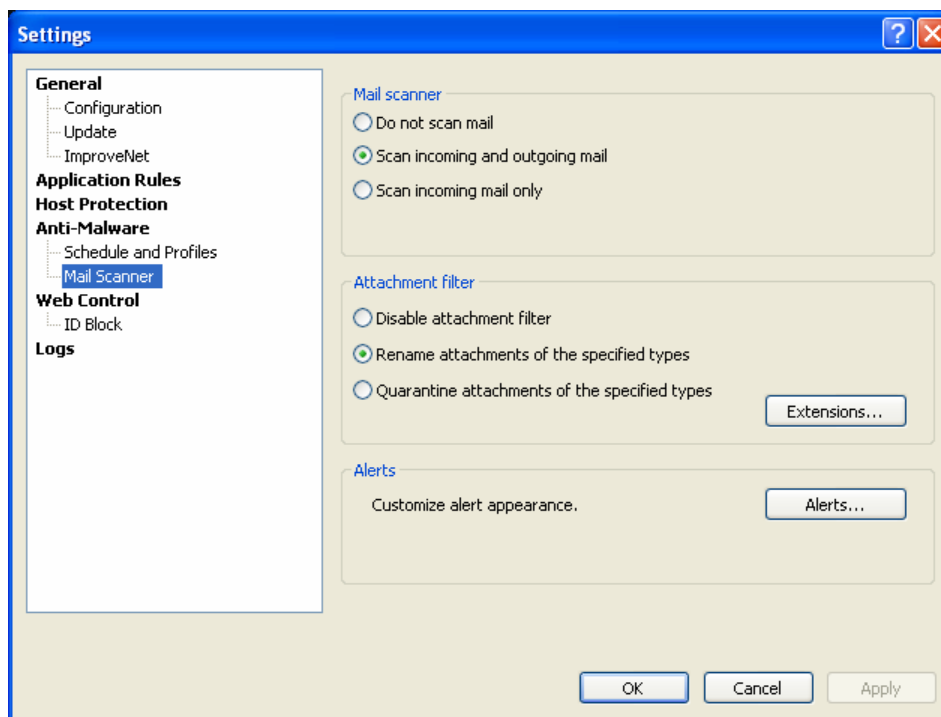
Note:

- 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.

6.3 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 starts performing its malicious actions resulting in system infection and malfunction.

Outpost Antivirus Pro protects you from attachments containing worms and Trojans, checking files attached to e-mail arriving to and being sent from your computer and quarantining those which Outpost Antivirus 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.

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 new malware 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 Antivirus 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 Antivirus Pro to show visual alerts and/or play sound alarms on detecting malware by clicking the **Alerts** button under **Alerts**.

Note:

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

6.4 Malware Quarantine

Outpost Antivirus 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 Malware. Objects in quarantine do not pose any threat to your computer.

Quarantined objects are displayed in **Quarantine** in the main Outpost Antivirus 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 malware 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 Antivirus Pro ignore it as spyware or simply omit during scans by selecting **Restore and Add Malware to Ignore List** or **Restore and Add File to Ignore List** correspondingly on the item's shortcut menu.

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

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.

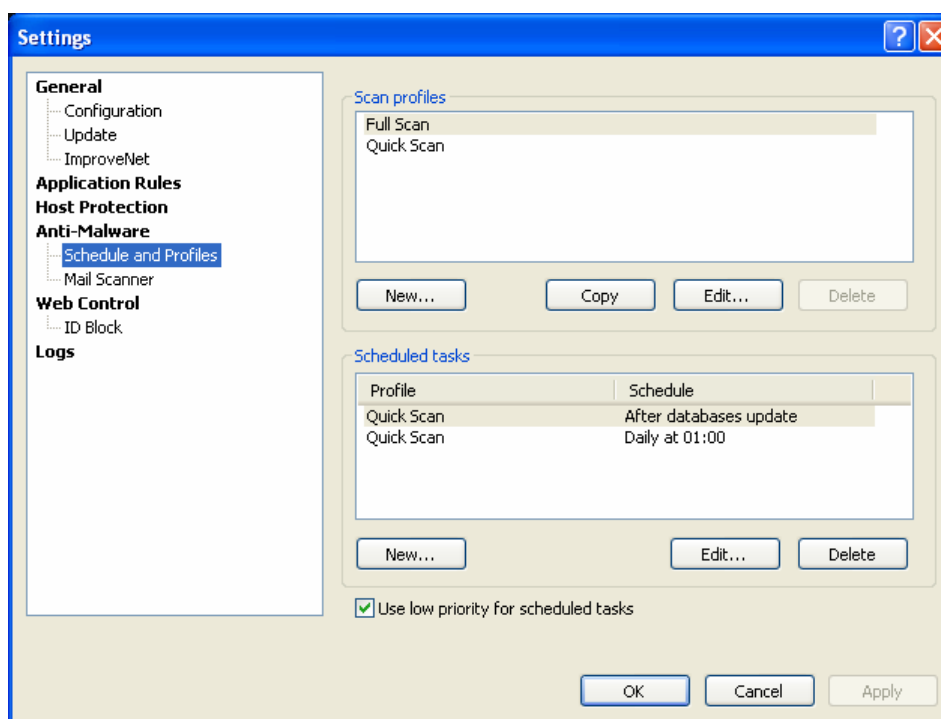
Note:

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

6.5 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 Antivirus 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 Antivirus 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**.

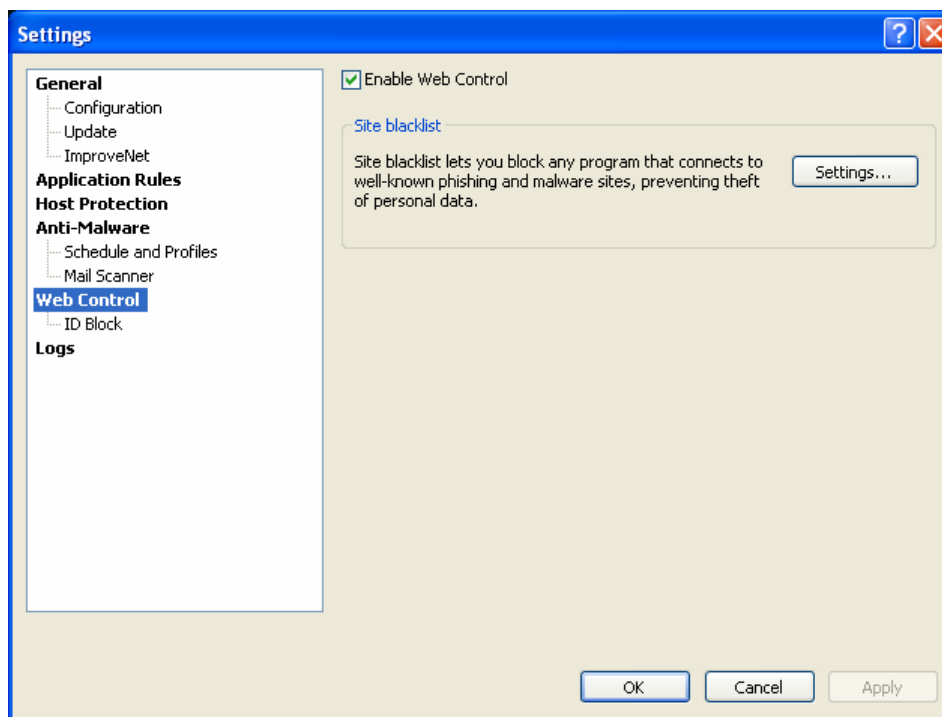
To save system resources at a time when the computer performs critical activity, select the **Use low priority for scheduled tasks** check box.

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

7 Controlling Online Activities

The versatile Web Control component 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, and keeps your identity private.

To activate the component, click **Settings** > **Web Control** and select the **Enable Web Control** check box:



7.1 Site Blacklist

Various sites on the Internet contain malware and they aim at spreading it among unwitting users. Outpost Antivirus Pro's database contains a list of such sites, access to which is not recommended unless you are eager to load malware 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 Antivirus Pro adds it to the visible list, which is available by clicking **Settings** > **Web Control** > **Settings** under **Site blacklist**.

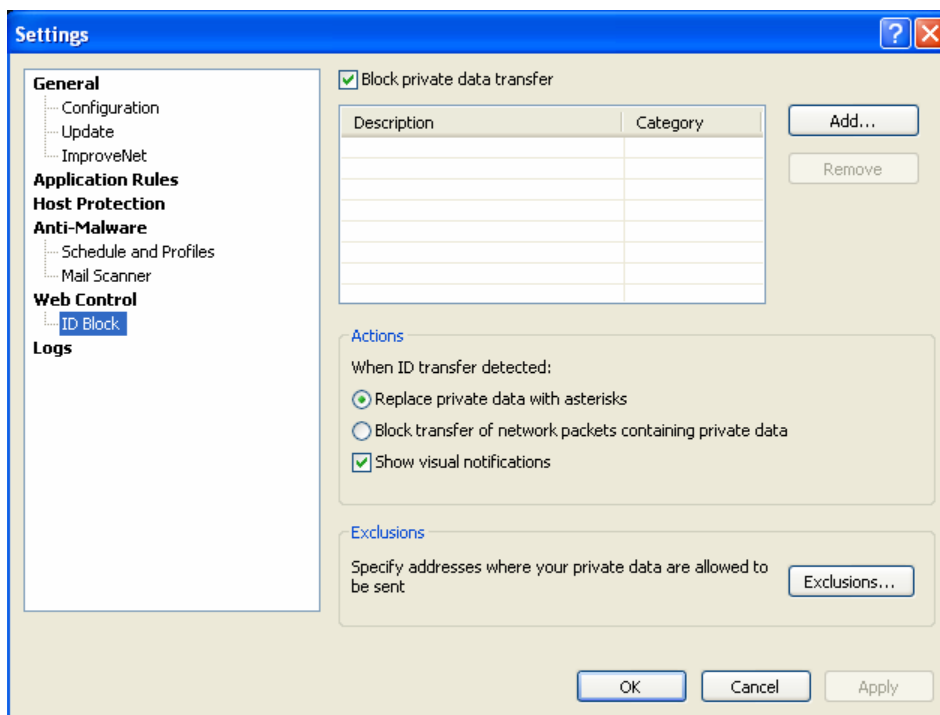
If there are any sites that you use or consider safe, you can allow access to them by clearing the corresponding check boxes.

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

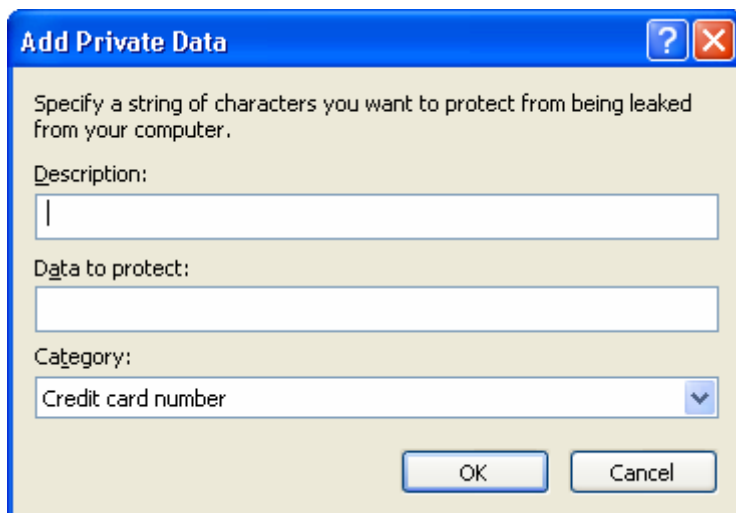
7.2 Blocking Private Data Transfers

Outpost Antivirus 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 Antivirus Pro can either **Replace private data 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 visual notifications** check box.

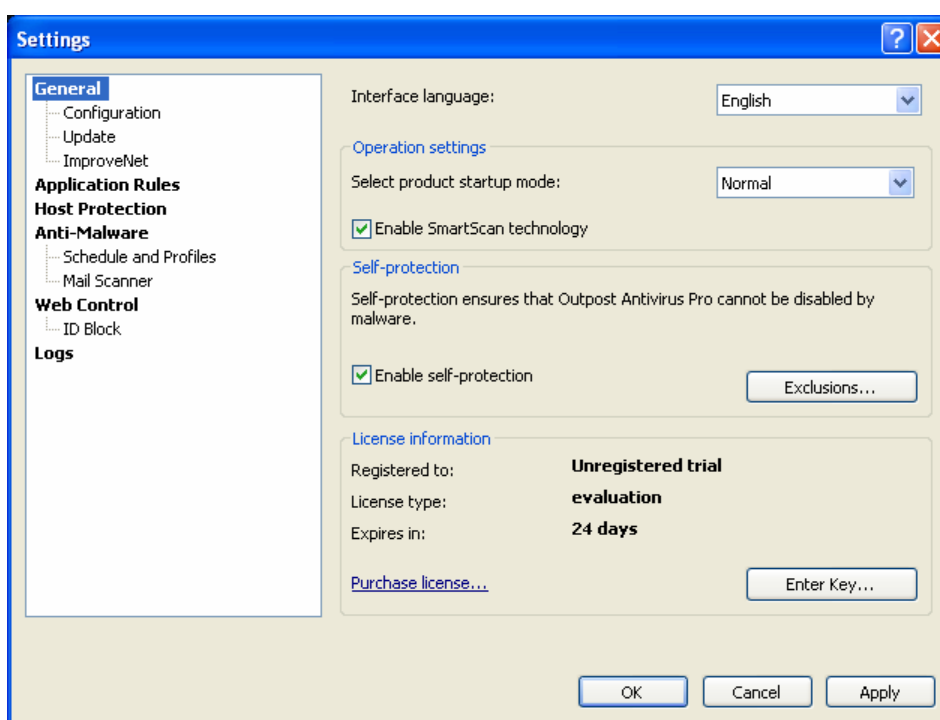
If you are certain that some hosts are trustworthy or they need to receive your private data, you can add such hosts to the exclusions list by clicking the **Exclusions** button. Specify the necessary site in the most convenient format for you, click **Add** and **OK** to save your settings.

8 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 Antivirus Pro features self-protection. With self-protection turned on, Outpost Antivirus Pro protects itself against termination caused by Trojans or Malware. Even attempts to simulate user keystrokes that would otherwise lead to Antivirus shutdown are detected and blocked. Outpost Antivirus 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 Antivirus 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 Antivirus Pro icon in the system tray and select **Disable Self-Protection**:



Note:

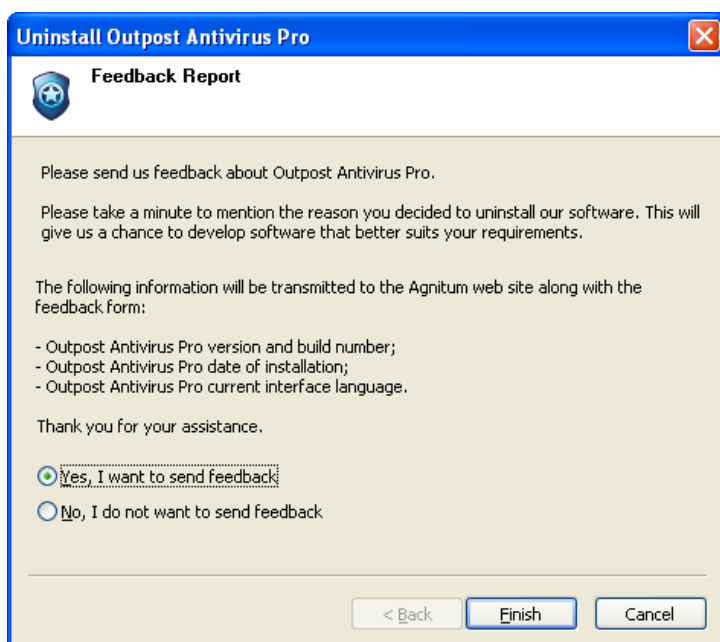
- Disabling self-protection may severely impact your overall system security. Though disabling is required for the installation of components and other advanced functions, it should be re-enabled as soon as the changes have been made.

9 Uninstalling Outpost Antivirus Pro

To uninstall Outpost Antivirus Pro:

1. Right-click the Outpost Antivirus 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 Antivirus 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.

10 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 Antivirus Pro, as well as the specific activities of each Outpost Antivirus Pro component, the start of each program and all changes made to configuration settings and passwords.

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 Antivirus Pro session.

The Event Viewer is accessed by double-clicking **Event Viewer** in the left panel of Outpost Antivirus Pro's main window. The set of the logs displayed depends on the current main window view. With the **Simple View**, the following logs are available (click the log name 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 program options and configuration settings.

- **Anti-Malware**

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

If you work with the Expert View of the main window, there are some more logs available:

- **Mail Events**

Displays the history of the incoming and outgoing mail and elements and attachments blocked. For information about mail scanner and attachment filter see [Scanning Mail Attachments](#).

- **Component Control**

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

- **Anti-Leak Control**

Displays the events of Outpost Antivirus 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.

10.1 Logging debugging information

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 enable logging of debugging information which can be useful for Agnitum's technical support service engineers to be able to resolve your issues.

To do this, 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 Antivirus 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.

11 Appendix

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

11.1 Troubleshooting

If you need assistance in working with Outpost Antivirus 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.

11.2 Understanding Penetration Techniques

By means of [Anti-Leak Control](#), Outpost Antivirus Pro allows you to control a lot of suspicious actions. For your convenience they are divided into 3 groups:

Win32 subsystem

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.pcinternetpatrol.com/>).

Outpost Antivirus 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, Malware, 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.Antivirusleak tester.com/leak test15.htm>). ZABypass is another example of a leak test that uses this method.

With Outpost Antivirus 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 Antivirus 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.Antivirusleak 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 Antivirus Pro controls such attempts.

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.pcfank.com/PCFlankleak test.exe>).

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

NT subsystem

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.Antivirusleak tester.com/leak test8.htm>, <http://www.Antivirusleak tester.com/leak test9.htm>).

Outpost Antivirus 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 Antivirus Pro (not just that of a network-enabled application). If malware tries to modify a legitimate application's memory, Outpost Antivirus 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-Malware 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 Antivirus. The example of using this technique is MBtest leak test (<http://www.Antivirusleak tester.com/leak test10.htm>).

Outpost Antivirus 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 Antivirus 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.

Keyloggers

Keyboard logging

Keyboard logging is a covert method of capturing and recording user keystrokes. Hackers can use this method through special keyloggers, which is software to illegally obtain passwords, keys and other sensitive information, which you type on your keyboard. Outpost Security Suite Pro detects attempts of any programs to record and transfer typed in information, thus protecting your computer from any data leakage.

11.3 Using Macro Addresses

Outpost Antivirus 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 Antivirus 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 Antivirus 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