

Quick Start
Guide

Outpost Security Suite 2007

Personal Security Software

from

Agnitum

Abstract

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

See the User Guide for detailed information on using Outpost.

Table of Contents

Table of Contents	3
Getting Started	4
Installing Outpost	4
Running and Shutting Down	4
Initial Options	5
Language	5
Operational Modes	6
Rules Wizard	7
Automatic Updates	8
Advanced Settings	9
Safeguarding Your System	9
Protection from Viruses and Spyware	11
Junk E-Mail Filtering	15
A Web Site's Hidden Programs	18
Ad Blocking	20
Content Blocking.....	22
Setting a Password	24
Technical Support	25

Getting Started

Installing Outpost

VERY IMPORTANT WARNING! Shutdown and uninstall any other security software before installing Outpost on your computer. Trying to install a suite over other running security software will crash your computer. Like a car with two drivers, each tries to steer and this will result into an accident!

Once you are certain no other security software is operating on your computer, install Outpost by running the installation package. It is recommended that you use the default settings when the installation utility asks you to confirm its choices if you are not an advanced user.

Note: See the [Maintenance Guide](#) for details on installing Outpost Security Suite.

Running and Shutting Down

As soon as it is installed Outpost Security Suite is already configured to work best for most users so it is perfectly safe just to close its window and let it do its job of guarding your computer.

One of Outpost's default settings is for it to run automatically when you start up Windows. This ensures your computer is protected at all times. If you prefer, you can change this setting so that Outpost does not start automatically. In this case, you will need to start Outpost manually each time to have it guard your computer.

To **start** Outpost manually:

1. Click on the Windows' **Start** button.
2. Move the cursor to **Programs**.
3. Select the folders **Agnitum**, then **Outpost Security Suite**.
4. Click on **Outpost Security Suite**.

To **shutdown** Outpost:

1. Right-click the Outpost icon in the system tray.
2. Select **Exit**.

Initial Options

Language

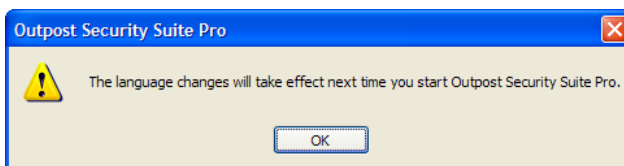
If you prefer a language other than English, the first thing to do is:

1. Double-click the Outpost icon on the taskbar. Outpost's main window is displayed:



2. Click on the **View** menu at the top of this window.
3. Select **Language** from this menu.
4. Choose your language from the list that's displayed.






You will see this message informing you that you'll need to restart Outpost before the new language takes effect:



Operational Modes

Outpost gives a wide choice of protection levels all the way from totally blocking all Internet access of every application on your computer to allowing full access to every application. For your convenience, Outpost has different operational modes to conform to the protection level you prefer.

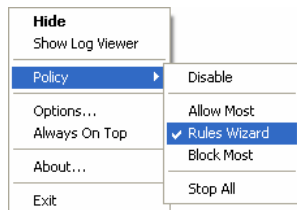
The operational modes are:

-  **Block all**—All network connections are disabled.
-  **Block most**—All network connections are disabled except those apps you enable.
-  **Rules Wizard**—You enable or disable apps when they are first run.
-  **Allow most**—All network connections are enabled except those apps you disable.
-  **Disable mode**—All network connections are enabled.

The default mode is **Rules Wizard**.

To change the operational mode:

1. Right-click on the system tray icon.
2. The following menu appears. Go to the **Policy** and select the operational mode by clicking on it.



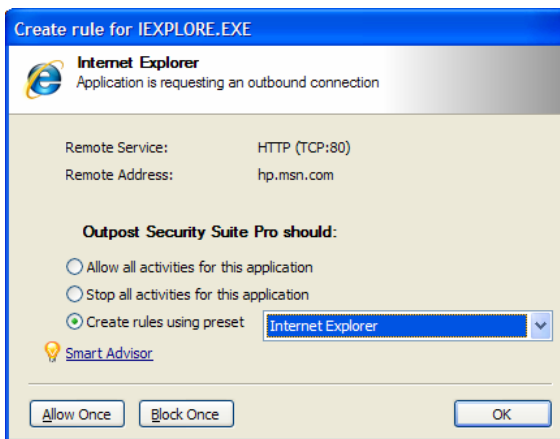
Rules Wizard

Rules Wizard is the operational mode that lets you decide each application's permissions to use the Internet. Outpost asks you whenever an application first tries to send or receive data. Rules Wizard is the default operational mode and is recommended for most users.

You can choose to make a rule for an app. If a rule is made then Rules Wizard is not displayed again for that app. If no rule is made for an app then Rules Wizard will display again the next time that app tries to send or receive data.

Don't be concerned about setting rules for apps. You can easily change or delete an application's rules at any time.

This is the Rules Wizard dialog:



It shows you the application (Internet Explorer, in this example), whether the app wants to send or receive data, the type of service the app is attempting to establish and the address the data is about to go to or be received from.

You are then given the following choices:


- **Allow all activities for this application**—For applications you trust completely. The application is then included in the **Trusted applications** list. (See **Options** menu, **Applications** tab.)
- **Block all activities for this application**—For applications which you know should not have network access. The application is included in the **Blocked applications** list. (See **Options** menu, **Applications** tab.)

- **Create rule using preset**—Outpost Security Suite lets you create rules using presets for most common applications or the presets that best suit an application (Internet Explorer, in our example above). Outpost is designed to offer the preset that best suits your application. The application will be included in the **Partially allowed applications** list. (See **Options** menu, **Applications** tab.) It is recommended that you select the preset offered by Outpost, however advanced users can click on the drop-down menu and select other presets or even create their own rule sets by selecting **Other**.
- **Allow Once**—For applications of which you are doubtful. The next time this application tries to establish a network connection, the same warning is displayed. No rule is created for the application.
- **Block Once**—For applications of which you are uncertain and distrust. The next time this application tries to establish a network connection, the same warning is displayed. No rule is created for the application.

Automatic Updates

Outpost can update itself automatically from Agnitum web site. This ensures that you get maximum protection from the latest threats discovered to be going around. Once a day, Outpost checks the site for an updated version of itself and if there is one it is downloaded and installed on your computer. You are notified each time this happens and can cancel the update if you prefer.

If for some reason you need to turn off automatic updating, click on Outpost's **Tool** menu then on **Automatically Check for Updates** to remove the checkmark.

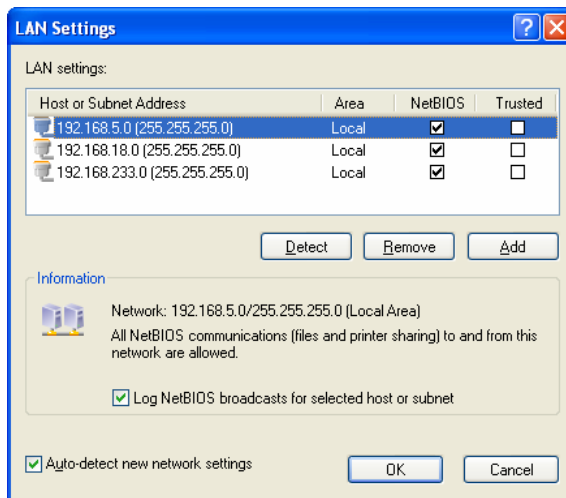
You can manually check for an update at any time by clicking on **Run Update** in the right-side panel or on the  button on the toolbar and following the wizard steps.

Advanced Settings

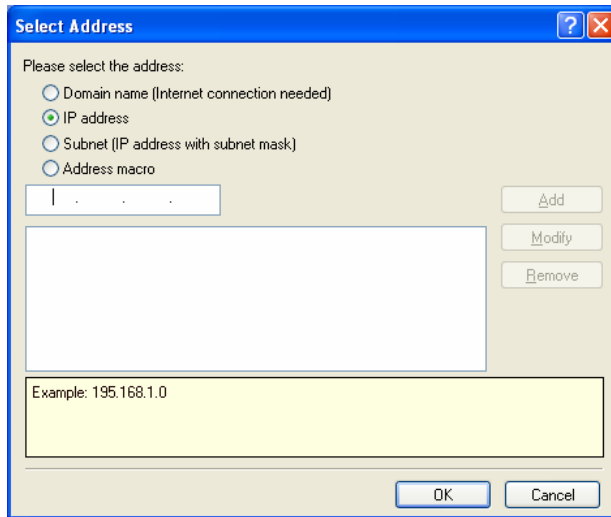
Safeguarding Your System

Outpost's settings for maximum protection:

- **Rules Wizard** mode informs you of any program trying to send data to or from your computer.
- **Stop all** mode prevents any data from being transmitted to or from your computer and Internet. Switch to this mode when you are absolutely certain that you don't need to access Internet resources, but still want to stay connected to the Web.
- Make your computer invisible to hackers. Click on the **Options** menu, then on the **System** tab. Select **Stealth** in the **Firewall mode** field.
- Ensure **NetBIOS** is turned off (disabled) unless your computer is on a local network and needs to share its files. If you need to use **NetBIOS** press the **Settings** in the **LAN Settings** field and make sure **NetBIOS** is selected for your local network like shows the picture below:



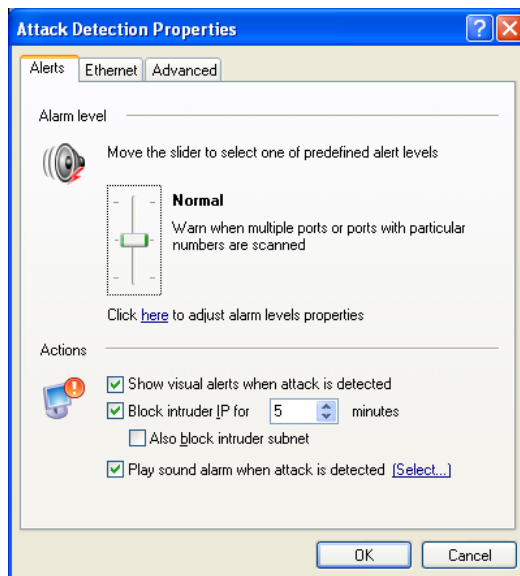
Click **Add** to add a remote computer or network to the list of allowed NetBIOS communications. The following dialog will be displayed:



To add a specific computer to the list, you must know its IP-address. Type in either the domain name, IP-address, or subnet mask into the corresponding field. Each option suggests the required format.

Please note that you must pay attention to this option because allowing unrestricted NetBIOS communications may result in severely decreased system security level.

- On the **Options** menu, click **Plug-Ins** and select **Attack Detection**. Click on the **Settings** button, then set the required options:



Note: You can see the Internet address from which your computer is being attacked in the **Outpost Log Viewer**. To open the Outpost Log Viewer for a specific plug-in, click on the plug-in icon in the Outpost left panel and then press the **Show Detailed Log** button in the information panel. The User Guide covers these logs in detail.

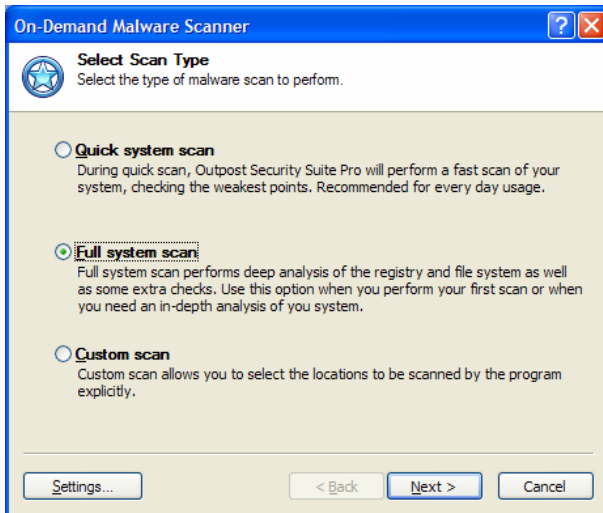
Protection from Viruses and Spyware

Anti-Malware plug-in is designed to prevent you from unwanted and unauthorized actions performed by malware. Both antivirus and anti-spyware capabilities are provided through the universal plug-in to ensure that your computer is kept clean of any malicious program that might infect while you're surfing the web.

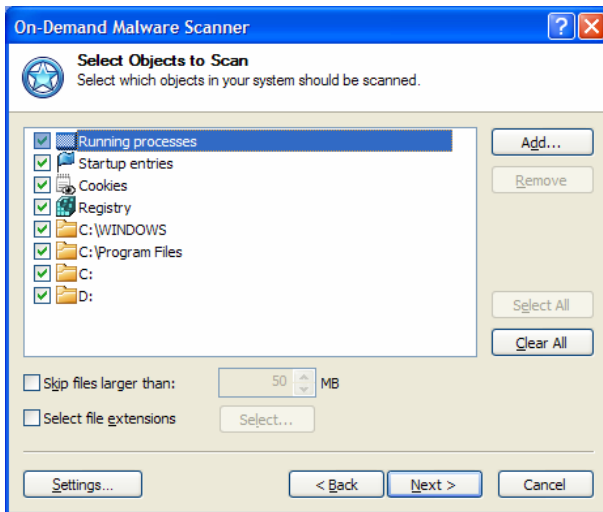
It is recommended to run a full scan just after Outpost Security Suite installation to check the system for whatever malware it already has on it. To do this, start On-Demand Malware Scanner by selecting the Anti-Malware plug-in in the tree and then clicking the **Run System Scan** button in the Information Panel. The wizard will help you specify the scanning settings and guide you through the whole process of the system scan.

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

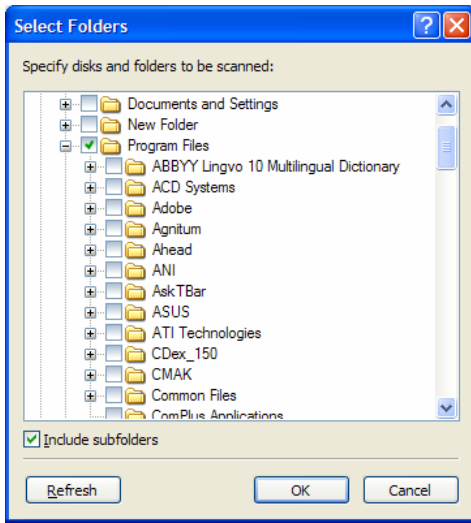
- **Quick system scan.** This option performs a fast scan of your system by checking only the most vulnerable points (such as running processes in memory, susceptible registry keys, target files and folders). This option is recommended for every day usage.
- **Full system scan.** A full system scan is 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 a 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 select the locations to be scanned explicitly. You can select either of the options above or you can choose specifically what to scan on your file system.



If **Custom scan** is selected, the **Select Objects to Scan** step appears allowing you to explicitly select the objects, disks, folders, and files to be scanned.

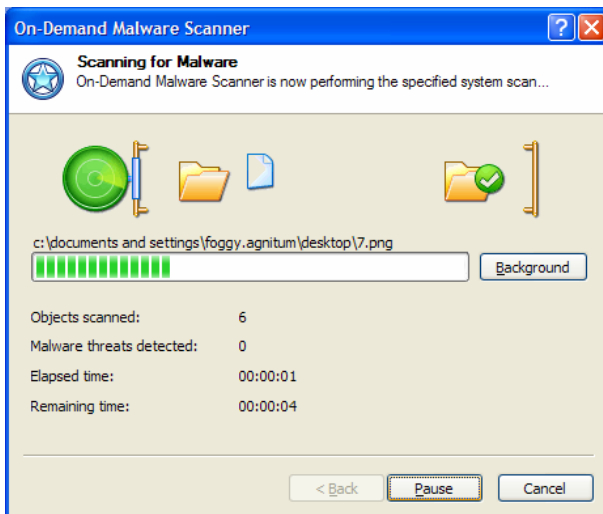


To add a folder to the list, click the **Add** button and in the **Select Folders** window, browse to and select the particular locations. Click **OK** to add the folders. To remove the selected object, click **Remove**.



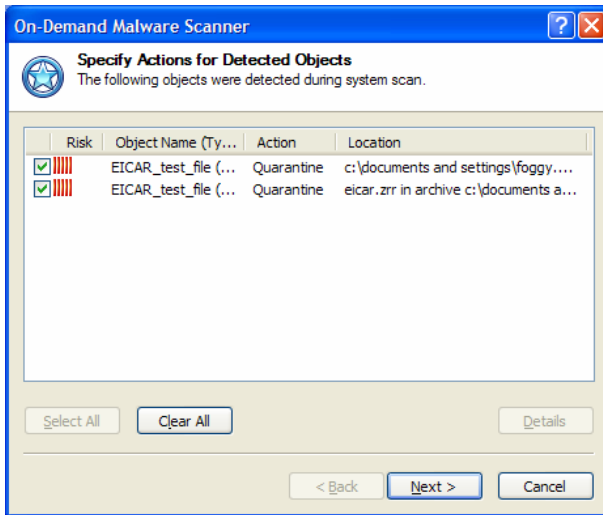
Once you have specified the objects and locations to scan, click **Next** to start the process.

Outpost Security Suite Pro starts to scan the selected objects and locations. The progress step displays the scanning current status and stats: the total number of objects scanned and the number of detected potentially malicious objects. When the scan is complete, a list of detected objects (if any) is displayed automatically. If your system is clear (i.e. no suspicious objects are found), just the stats of the scan are displayed.



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

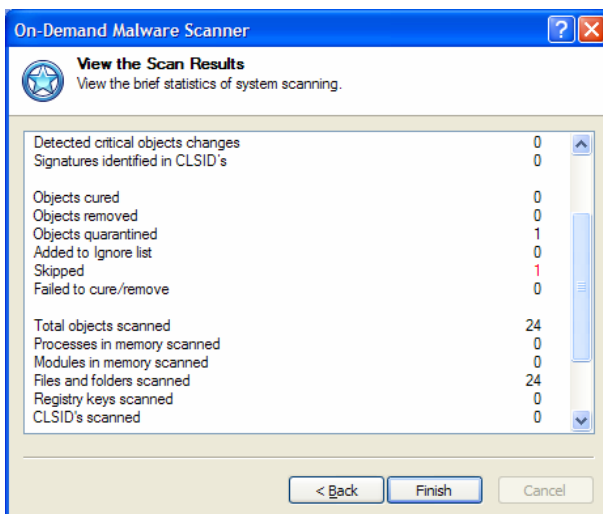
To change the action, right-click the object and select the action from the shortcut menu.



Select the check boxes next to objects you want to process and click **Next**. Outpost Security Suite Pro then performs the specified actions—cures the object, removes it from the places it is registered in and from memory or places in quarantine so you can restore it later if you find your favorite software won't work without it or you can delete them completely if all is well. While in quarantine, malware has no effect on your system.

The software that you did not select will be left intact and will continue their activity in your system.

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



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

To enable the real-time protection, open the plug-in properties by right-clicking the plug-in in the tree and selecting **Properties** and select the **Enable real-time protection** check box. You can also set the real-time protection operation mode. Select **Check files on execution** if you want to prevent known malware from execution, but don't want to prevent other access attempts such as copying or saving malware samples. Or select **Check files on every access attempt** and Outpost Security Suite Pro will prevent all access attempts to files infected by known malware. Note, that the last mode can affect system performance.

Junk E-Mail Filtering

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

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

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

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



To enable or disable spam filtering in either Microsoft Outlook or Microsoft Outlook Express mail client, right-click the plug-in in the Outpost Security Suite Pro main window and select the corresponding command.

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

There is also a non-statistical way that Anti-Spam immediately gets to work marking letters as "not spam". These are e-mails from people on your Contacts list, people you write to and your own outgoing e-mail. These messages are the only ones the filter handles before its training stage is finished. To collect a really valuable knowledge base, Anti-Spam needs some training.

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

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

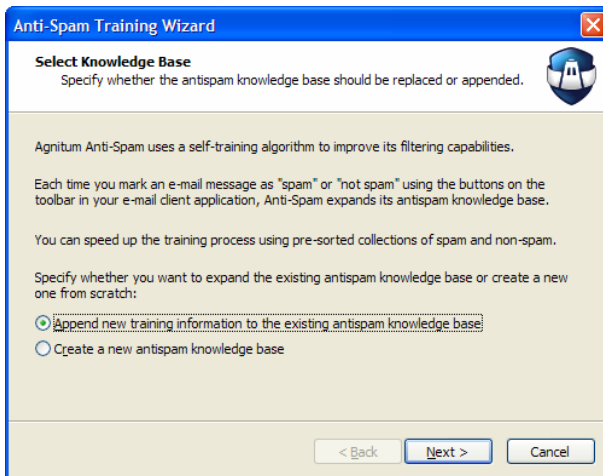
This method is relatively slow because the filter processes e-mails after they have been received. However, after some time the filter will enlarge the knowledge base so he can precisely detect spam without any false positives.

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

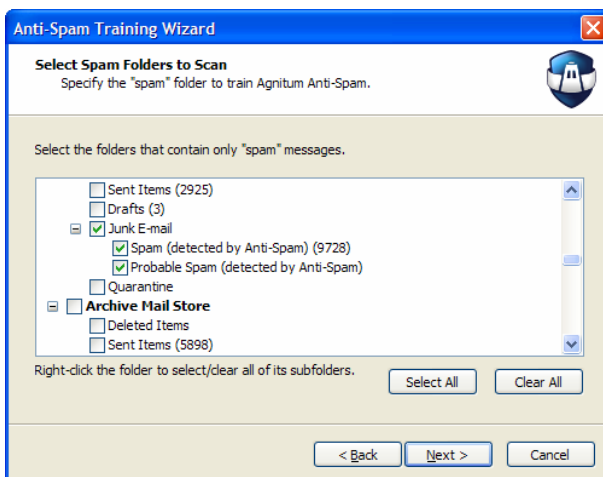
Note: During training (especially at the beginning, when the collected statistics are small), it is recommended that you periodically check the junk-mail folder and if you find any e-mail

mistakenly detected as spam, mark them as "not spam" using the **Mark as Not Spam** button on the toolbar.

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



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



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

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

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

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

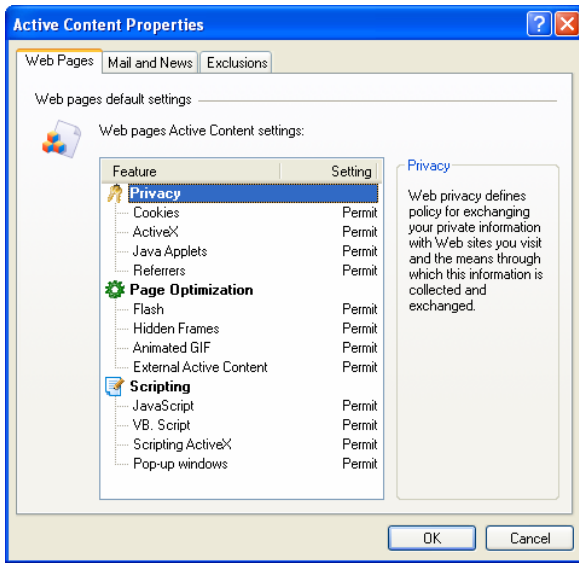
A Web Site's Hidden Programs

A web site can use programs to make its pages more interesting or useful. Examples include animations, calendars, specialized calculators and helpful menus. Most of the time these embedded programs perform a useful or aesthetic function.

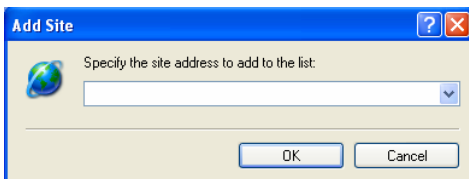
However, some hackers found ways to make embedded programs destructive so Outpost gives you the option of disabling each questionable component individually. To do this:

1. Double-click the icon in the system tray to display Outpost's main window.
2. Right-click on **Active Content** to show its shortcut menu:

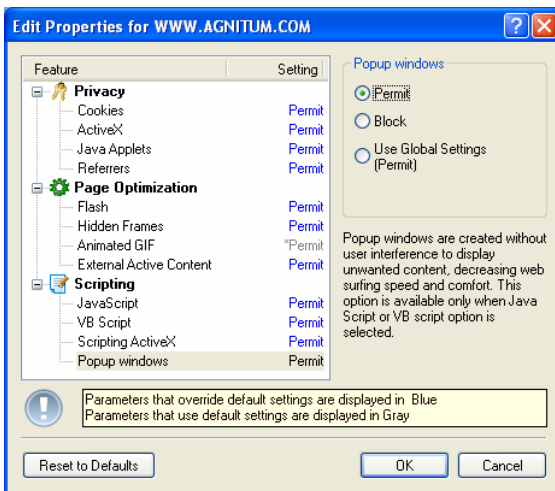
Clicking on **Properties** shows you the dialog with the list of web pages active content:



This dialog lets you configure the default active content settings that apply to every web site you visit. To specify settings for an individual site select the **Exclusions** tab, then click on the **Add** button and enter the site's address.



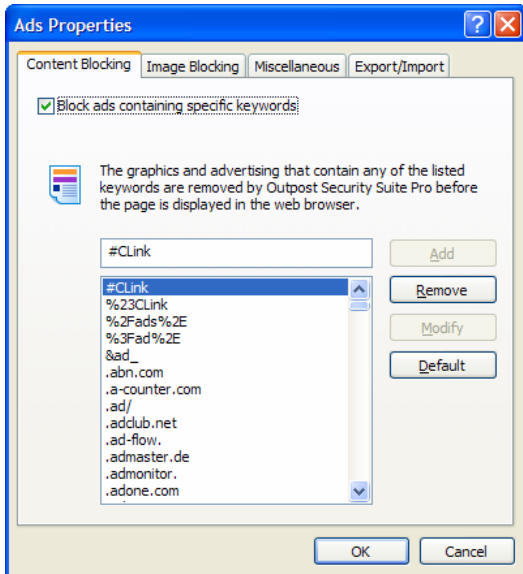
After the site is added to the exclusions list you can configure the active content settings that will apply to that site only.



Ad Blocking

Advertising pays the expenses of many web sites so they can give their info or software away for free. However, often ads greatly slow down the connection, are offensive and/or simply irritating.

To have Outpost block ads on the web pages you are browsing, right-click on **Ads** under **Plug-Ins** in the left panel. Then select **Properties** to get the following dialog:

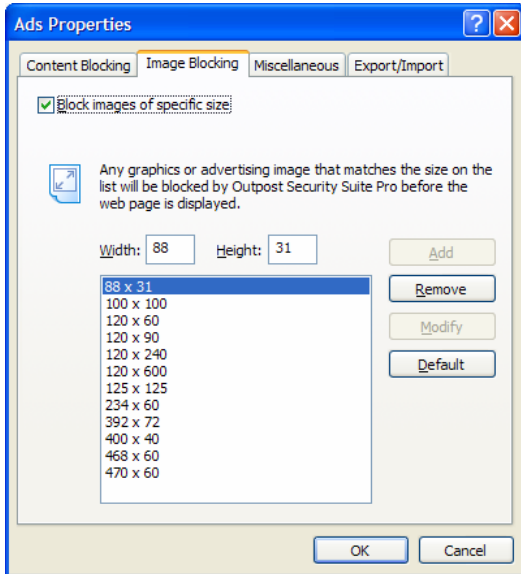


Ensure the **Block Ad content containing specific keywords** checkbox is checked.

To add an address to the list of ad servers, enter it in the field above the list and click the **Add** button. To edit an address, select it on the list, then edit it in the field above the list and click the **Modify** button. To delete an address, select it and click the **Remove** button.

The **Default** button restores the list to what it was when Outpost was first installed.

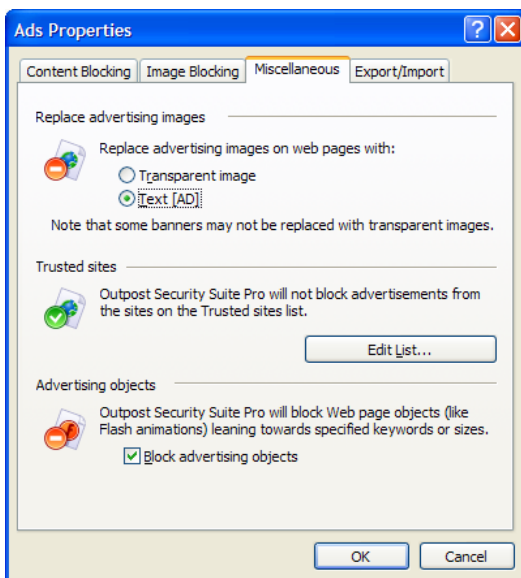
To prohibit ads of specific sizes click the **Image Blocking** tab to get this dialog:



Configure the settings the same way you did in the previous window.

Note. Blocking ads by image size blocks the display of all images of standard size *that are links* (i.e. within anchor `<a>` tags), whether they are linked to another site or simply to another page on the same site.

Outpost Security Suite also allows you to specify whether to replace advertisements with text message **[AD]** or with **transparent images** the same size as the ad. Click the **Miscellaneous** tab to alter these settings:



Note: Some banners cannot be replaced with transparent images and will be replaced with text messages regardless the option specified.

Please note that Outpost Security Suite blocks banner ads according to the settings you specify. Some legitimate images could be blocked if the setting is too strict, such as adding the word “image” to the list of blocked words.

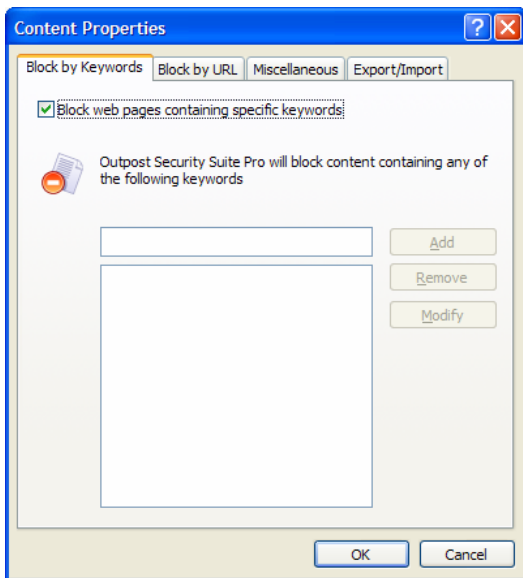
In the case when ad blocking prevents you from browsing the specific web sites, you can put these sites on the **Trusted sites** list. Outpost does not block advertisements on the trusted sites. To add a site, select the **Edit list**, specify the site address and click **Add**.

Outpost Security Suite can also block advertisements that are represented by various Web page ActiveX objects thus saving your system resources and traffic bandwidth. Select the **Block advertising objects** to enable this advertisement filtering.

Content Blocking

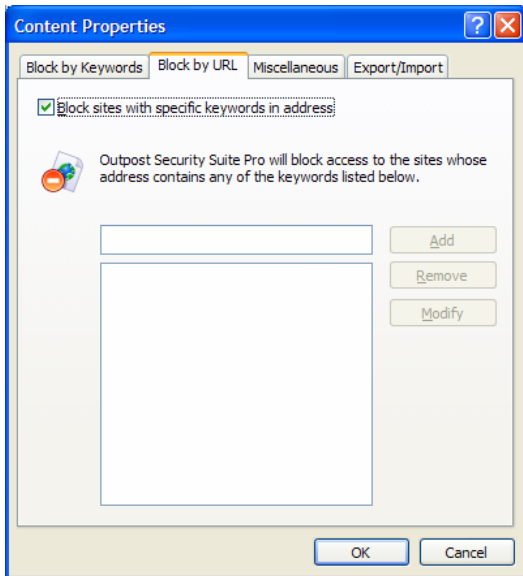
Outpost can block specific web sites as well as any web page that contains a word or phrase you specify.

To have Outpost block objectionable content, right-click on **Content** in the left panel of Outpost’s main window and select **Properties** to get this dialog:



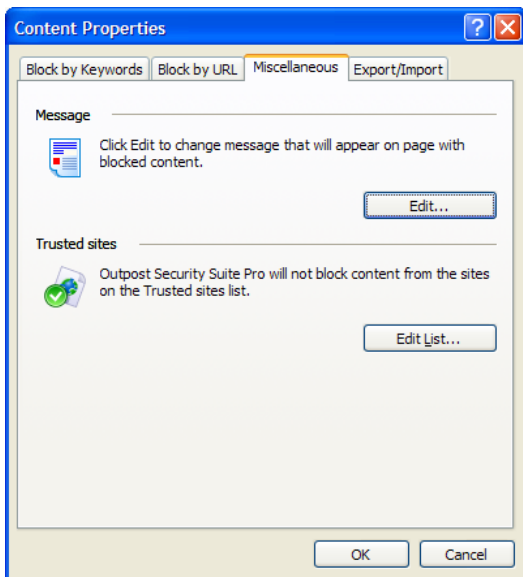
The settings in this window are pretty much the same as for the **Ads** filter.

To list particular web sites you do not want displayed on your computer, select the **Blocked Sites** tab.



Populate the list the way you did for the ad blocking.

To change the message that will appear instead of pages with objectionable materials click **Miscellaneous**.

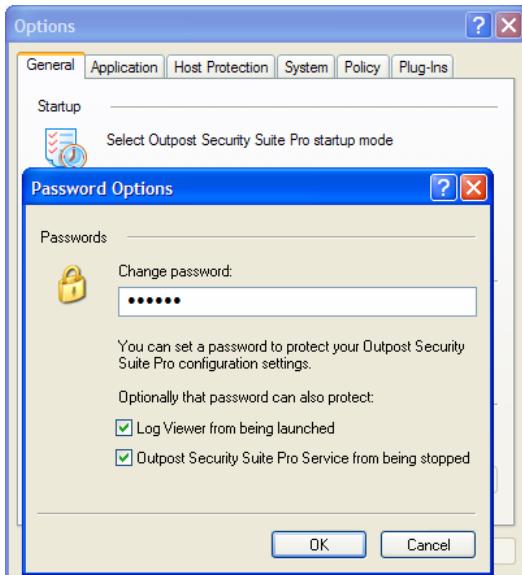


Click **Edit**, type in the message, and click **OK** to save.

Setting a Password

If you have children and don't want them to change the settings you made, you can set a password for Outpost.

This is done from the **Options** dialog by selecting **Enable** in the **Password protection** field as shown here:



Specify the password and opt whether it should protect the firewall settings only or should prevent Log Viewer from being launched and/or Outpost service from being stopped as well. Click **OK** and confirm the password in the dialog box appeared.

Technical Support

If you need assistance in using Outpost, visit its support pages at <http://www.agnitum.com/support/> page for available support options including knowledge base, documentation, support forum, product-related web resources, and direct contact with support engineers.