

Quick Start
Guide

Outpost Client Firewall

Personal Firewall 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 Client Firewall 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
Some Background	4
Internet Basics	4
Why Outpost Client Firewall is Needed	4
The Main Threats	5
How Outpost Client Firewall Works	5
Outpost Client Firewall's Features	6
Getting Started	7
Running and Shutting Down	7
Initial Options	8
Language	8
Operational Modes	9
Rules Wizard	10
Advanced Settings	12
Safeguarding Your System	12
A Web Site's Hidden Programs	14
E-Mail Threats.....	16
Ad Blocking	18
Content Blocking.....	20
Technical Support	22

Some Background

Internet Basics

The Internet is interactive, which simply means that when a computer is connected to the Internet, data can be sent and received by that computer to other computers on the Internet. This interactivity is built into the Internet and is a fundamental part of it.

To see a web site on the Internet, your computer basically asks that site for its files. The site's computer (server) then sends (serves) those files to your computer. For the files to get from the server all the way through the Internet over to your computer, your computer must give the site's server your computer's address. This address is unique and called IP address. No other computer on the Internet has this same address.

The Internet uses what's called a server-client way of doing things. Web sites use servers to supply their web pages and people use their computers as clients that are served those pages. The vast majority of information on the Internet goes from the servers to the clients, from the web sites to the desktop computer. Very little information goes from your computer back to the server.

Why Outpost Client Firewall is Needed

The major reason Outpost is needed is because a small percentage of Internet users are destructive. These people are called hackers or crackers. Traditionally a hacker is an accomplished computer programmer who is an expert in networks. A cracker is the term for someone who gains unauthorized access to a computer or system. The news media has blurred these definitions and refers to anyone who breaks into other people's computers as a hacker.

It used to take some skill to crack into a system but nowadays there are programs that can do it automatically. Children without much training or expertise can use them. These programs can be gotten effortlessly from the Internet. Many of these programs are sent around the Internet haphazardly as attachments to e-mails. Once the program is running on a user's machine, it "calls home" to a central site and reports where it is. The hacker can then control that user's machine remotely without the user even being aware of it. The hacker can record all the keyboard actions and mouse movements of the user's computer so can capture credit card data and passwords with ease. Sounds like science fiction but it is very much a cold, hard fact.

Another undesirable element of the Internet is the ever-present threat of computer viruses that are disseminated through email. These are so numerous that if something goes wrong with a computer the first thing suspected (and often discovered) is a virus.

Advertiser tracking of your surfing habits and interests has recently become a concern of privacy advocates. Advertisers use the data they gather on you to push specific ads calculated to increase your purchasing.

The Main Threats

- Someone on the Internet thousands of miles away can access your computer and personal files more easily than your neighbor down the street.
- Once your computer is accessed, all of its files can be viewed, copied and erased.
- Your computer can be used to attack other innocent user's computers without your knowledge.
- A hacker can very easily make your Internet connection totally unusable just for kicks.
- Your passwords, credit card info, house address can all be obtained remotely very easily.
- Unscrupulous advertisers can track your surfing habits, your interests and your locale, thereafter target specific ads at you.
- Personal info about you can be collected for various reasons, all without your knowledge or consent.

How Outpost Client Firewall Works

Outpost is a firewall, the technical name for a barrier between your computer and the rest of the Internet. It's like the locks on the doors of your home. Most of your neighbors can probably be trusted not to walk into your home and vandalize it or steal from you. Usually only a small number of your neighbors are untrustworthy. But, if you live in heavily populated area, there are a greater number of dishonest people around.

The Internet is similar except that your immediate neighborhood consists of hundreds of millions of people. Even the small percentage of those people who have a destructive bent is a large number of people.

Outpost Client Firewall not only locks your computer's "doors", it makes your computer invisible on the Internet. Your computer normally lets other Internet users know its address. It's like the address sign of your home or the license plate of your car. Your computer's address is plainly visible. Outpost prevents your computer from broadcasting its address unless specifically

authorized by you. Hackers are not just kept out; they cannot find out that your computer is connected to the Internet.

Outpost Client Firewall's Features

- Starts protecting immediately after being installed.
- Has a default configuration setting for new users.
- During the installation auto-configures for optimum protection.
- Can be customized in detail by advanced users.
- Makes your computer invisible on the Internet.
- Locks your computer's "doors" ports against intrusion.
- Let's you decide how much an application should be trusted.
- Uses plug-ins to increase its power while keeping the same familiar interface.
- Stops Internet ads from distracting you or slowing your browsing.
- Prevents ad tracking of your surfing habits and interests.
- Prevents your computer from being controlled remotely.
- Notifies you of any hidden software attempting to "phone home" to a hacker.
- Runs on all recent versions of Windows so can still be used if you upgrade.
- Uses very little system resources so does not noticeably affect your computer's performance.
- Advanced Log System lets you view any event on your system.
- Successful on all known "leak-tests".
- Multi-language: Outpost Client Firewall supports 7 languages.

Getting Started

Running and Shutting Down

As soon as it is installed Outpost Client Firewall 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.

When Outpost Client Firewall is running its icon is placed in the system tray, on the right-hand end of the Windows task bar. If you do not see the Outpost Client Firewall icon in the system tray, then you know that Outpost Client Firewall is not protecting your computer *unless it is set up to run in background mode*.

To **start** Outpost manually:

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

To **shutdown** Outpost:

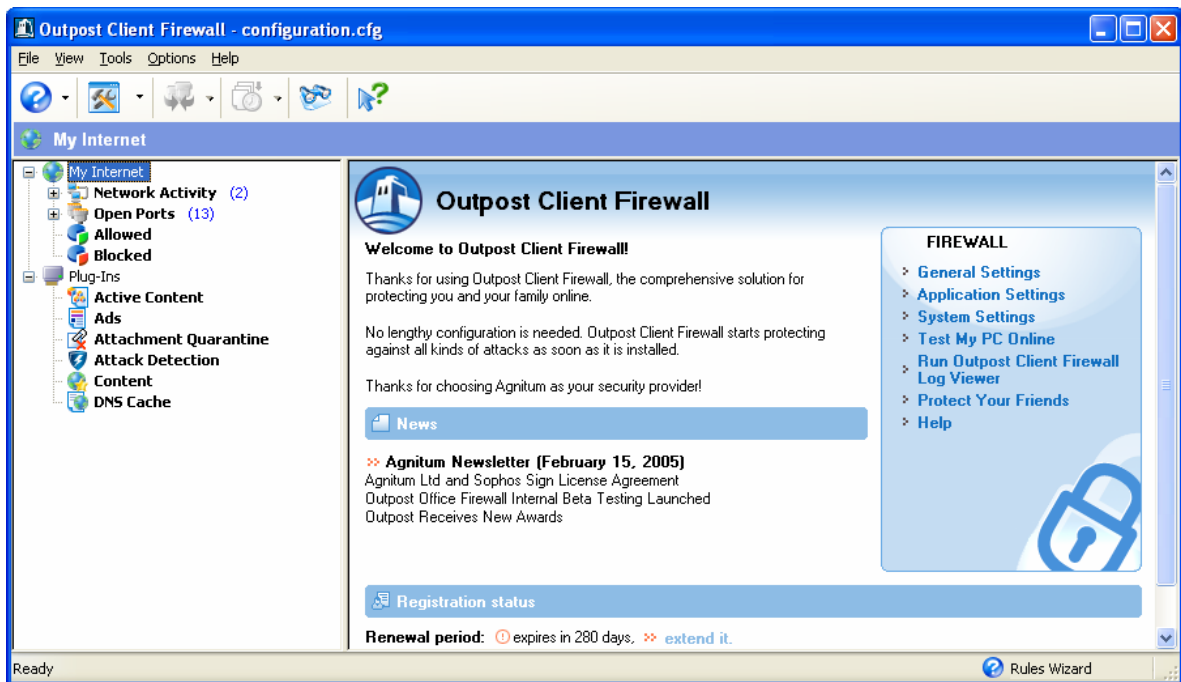
1. Right-click the Outpost icon in the system tray.
2. Select **Exit and Shutdown Outpost**.

Initial Options

Language

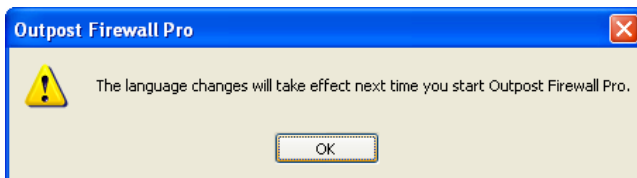
If you prefer a language other than English, the first thing to do is:

1. Double-click the 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

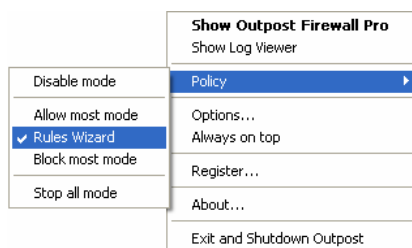
Outpost gives a wide choice of protection levels all the way from totally blocking all Internet access of every application on your computer to allowing full access to every application. For your convenience, Outpost has different operational modes to conform to the protection level you prefer.

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.

To change the operational mode:

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



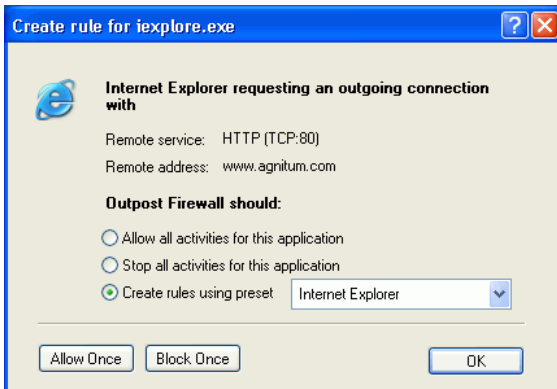
Rules Wizard

Rules Wizard is the operational mode that lets you decide each application's permissions to use the Internet. Outpost asks you whenever an application (app) 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 Client Firewall 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.

Advanced Settings

Safeguarding Your System

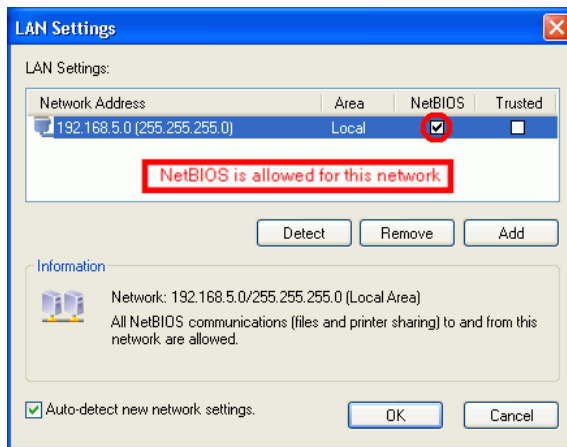
Trojan horses are the most dangerous threats to your computer files and your confidential information such as your passwords, credit card data and personal correspondence. A Trojan is a program installed on your computer that gives full access to hackers. The same Trojan can be used secretly by many hackers. It's not just one Trojan to one hacker. It's one Trojan to many hackers.

A Trojan on your computer can let a hacker view, copy or erase any folder and any file on your computer just as though he or she were sitting at your computer using its keyboard and mouse. Any file on your computer can also be sent to any e-mail address or posted on the Internet.

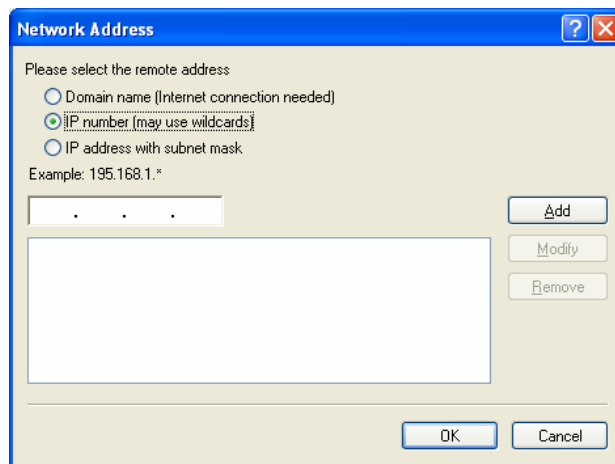
There are many ways a system can be infected with a Trojan and because a Trojan is not the same as a virus. It is a self-replicating program segment and it is not always detected by anti-virus software. Outpost was designed to nullify the malicious actions of Trojans.

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:



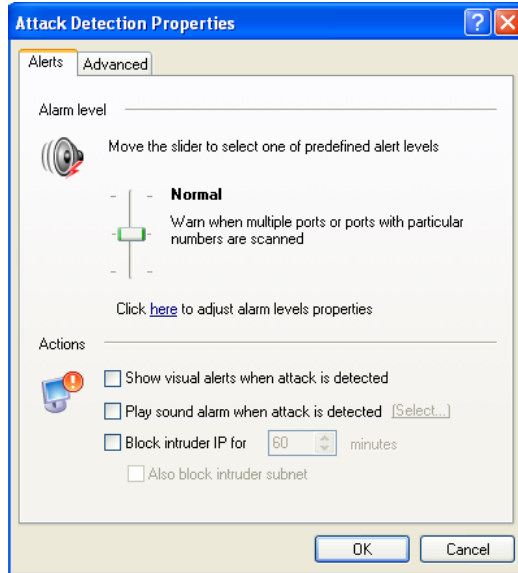
Click **Add** to add a remote computer or network to the list of allowed NetBIOS communications. The following dialog will be displayed:



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:




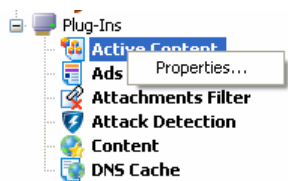
Note: You can see the Internet address from which your computer is being attacked in the **Outpost Log Viewer**. To open the Outpost Log Viewer for a specific plug-in, click on the plug-in icon in the Outpost left panel and then press the **Show Detailed Log** button in the information panel. The User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

A Web Site's Hidden Programs

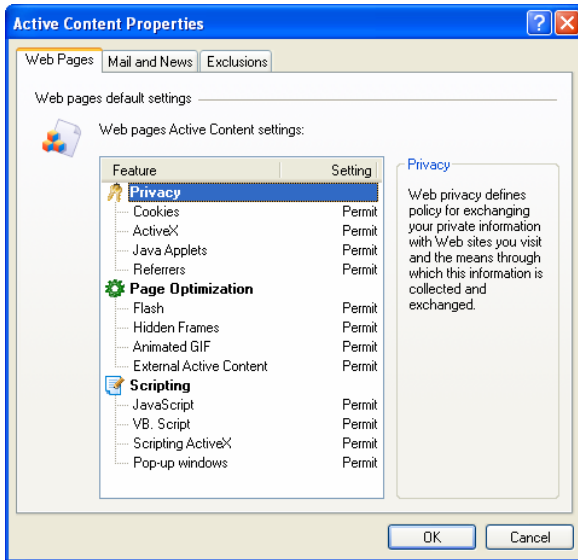
A web site can use programs to make its pages more interesting or useful. Examples include animations, calendars, specialized calculators and helpful menus. Most of the time these embedded programs perform a useful or aesthetic function.

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:

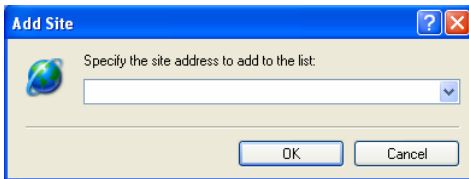
1. Double-click the icon  in the system tray to display Outpost's main window.
2. Right-click on **Active Content** to show its shortcut menu:



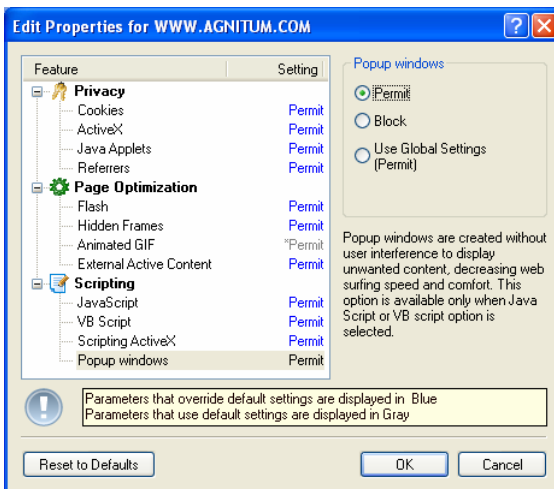
Clicking on **Properties** shows you the dialog with the list of web pages active content:



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.



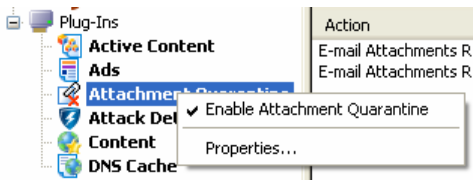
After the site is added to the exclusions list you can configure the active content settings that will apply to that site only.



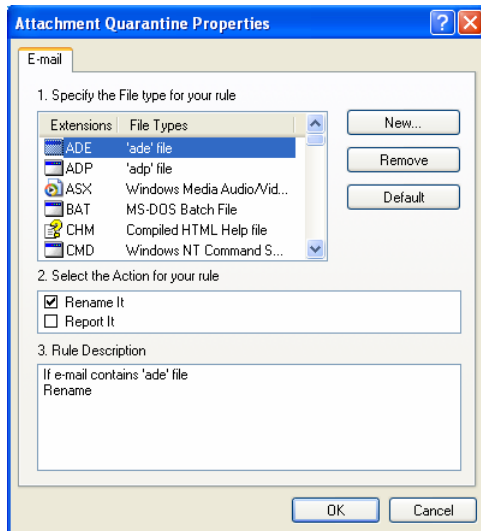
E-Mail Threats

Active content can be embedded in e-mails as easily as it can in web pages. Disabling these components for your e-mail is done the same as with web pages. See previous section for details.

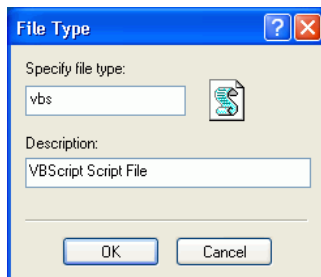
Another threat e-mail can bring to your computer are programs disguised as innocent e-mail attachments. This is a very common way of installing malicious Worms and Trojan horses, seemingly helpful programs that can crash your computer and/or open your computer system to direct hacker control. To safeguard against this, you can specify how Outpost should handle each type of file attachment. This is done by right-clicking the **Attachments Quarantine** and selecting **Properties** like this:



This gives you the following dialog:



The **New** button allows you to add file types to be inspected by Outpost:

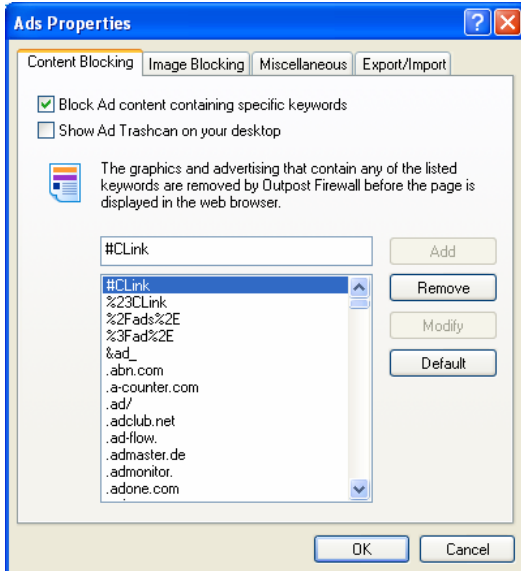


After adding the file, you need to select the action for Outpost Client Firewall to take when this file type arrives into your inbox as an email attachment. It is recommended that you choose **Rename It** to quarantine the file so you can safely save it to your hard disk and scan with anti-virus software before opening that attachment.

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:

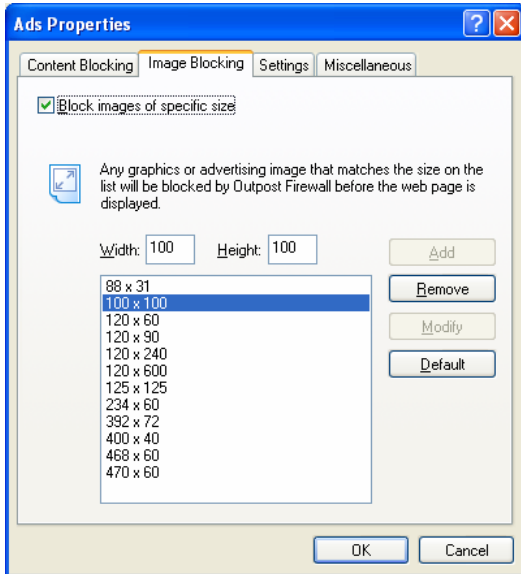


Ensure the **Block Ad content containing specific keywords** checkbox is checked.

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.

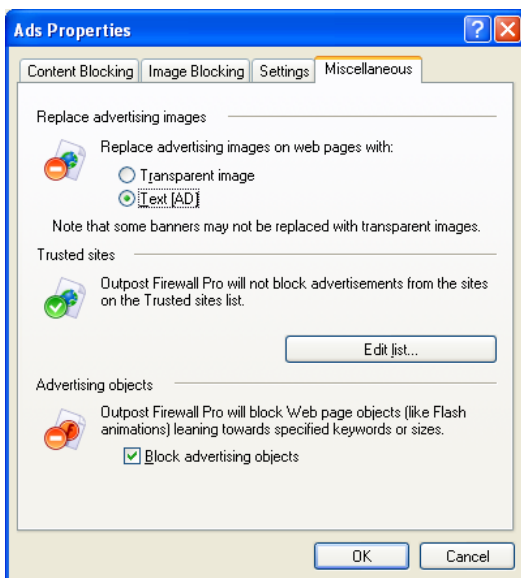
To prohibit ads of specific sizes click the **Image Blocking** tab to get this dialog:



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 Client Firewall 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 Client Firewall 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.

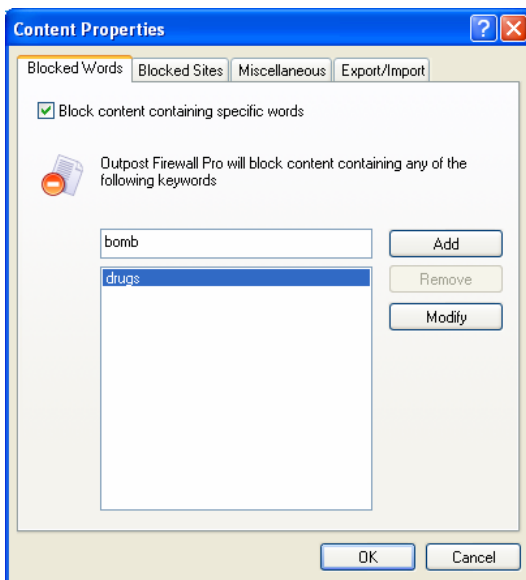
In the case when ad blocking prevents you from browsing the specific web sites, you can put these sites on the **Trusted sites** list. Outpost does not block advertisements on the trusted sites. To add a site, select the **Edit list**, specify the site address and click **Add**.

Outpost Client Firewall 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

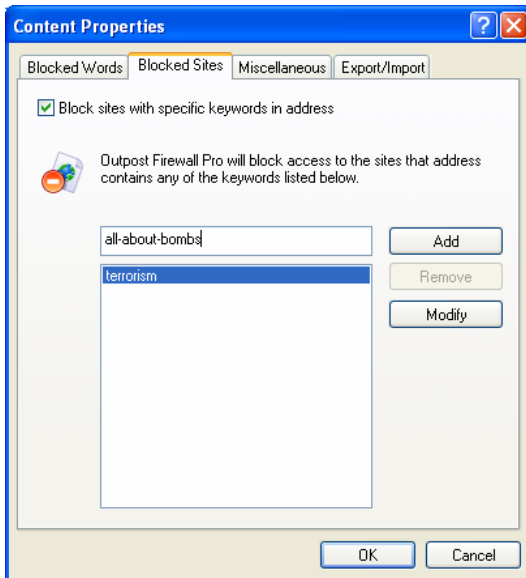
Outpost can block specific web sites as well as any web page that contains a word or phrase you specify.

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:



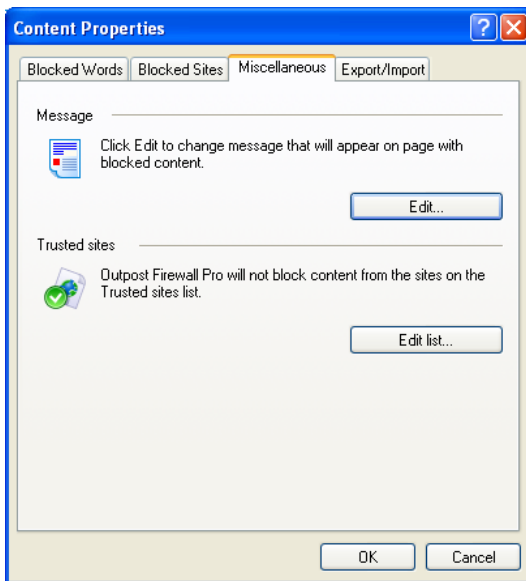
The settings in this window are pretty much the same as for the **Ads** filter.

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.

Technical Support

If you need assistance in using Outpost Client Firewall, visit its support pages at <http://www.agnitum.com/support/> page for available support options including FAQs, Documentation, Forum, Tips-n-tricks and Troubleshooting.