

Quick Start

Reference

Outpost Firewall

Personal Firewall Software

from

Agnitum

Scope of This Document

This is a quick start reference to orientate a first time user to the basic concepts and operations of Outpost firewall software.

It also gives some of the primary ways a user might want to customize Outpost to fit his or her preferences.

Further Reading

A much more detailed reference to Outpost is the User Guide.

Table of Contents

Some Background	4
Internet Basics	4
Why Outpost is Needed.....	4
The Main Threats	5
How Outpost Works	5
Outpost's Features.....	6
Getting Started	7
Installing Outpost	7
Running and Shutting Down.....	7
Initial Options	8
Language	8
Operational Modes	9
Rules Wizard	11
Automatic Updates.....	12
Advanced Settings.....	16
Safeguarding Your Files	16
A Web Site's Hidden Programs.....	20
E-Mail Threats.....	22
Ad Blocking	24
Content Blocking.....	26
Setting a Password	28
Trusted Zone.....	29

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 from one's own computer to other computers on the Internet. This inter-activity 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. 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 its 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 is Needed

The only 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 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 from the Internet without much trouble. 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, then target specific ads at you.
- Personal info about you can be collected for various reasons, all without your knowledge or consent.

How Outpost 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. There's only a fraction of your neighbors who are untrustworthy. But, if you live in a populated neighborhood, there is a greater number of dishonest people around.

The Internet is similar except 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 not only locks your computer's "doors", it makes your computer invisible on the Internet. Your computer normally is letting 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 can't tell your computer is there.

Outpost's Features

- Starts protecting immediately after being installed.
- Has default configuration settings for new users.
- Can be customized in detail by advanced users.
- Makes your computer invisible on the Internet.
- Locks your computer's "doors" (Internet ports) against intrusion.
- Let's you decide how much an application should be trusted.
- Advises new users with each selection they make.
- Advanced users can extend Outpost's capabilities.
- 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.
- Uses all 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.

Getting Started

Installing Outpost

VERY IMPORTANT WARNING! Shutdown any other firewall software before installing Outpost on your computer. Trying to install a firewall over other running firewall software will crash your computer. Like a car with two drivers, each firewall tries to steer and the computer runs into a pole!

Once you are certain no other firewall is operating on your computer, install Outpost by running `outpost.exe`. 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.

Running and Shutting Down


Outpost starts automatically as soon as it is installed. It 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. You can change this setting so Outpost does not start up automatically if you prefer. 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 Firewall 1.0*.
4. Click on *Outpost Firewall*.


To **shutdown** Outpost:

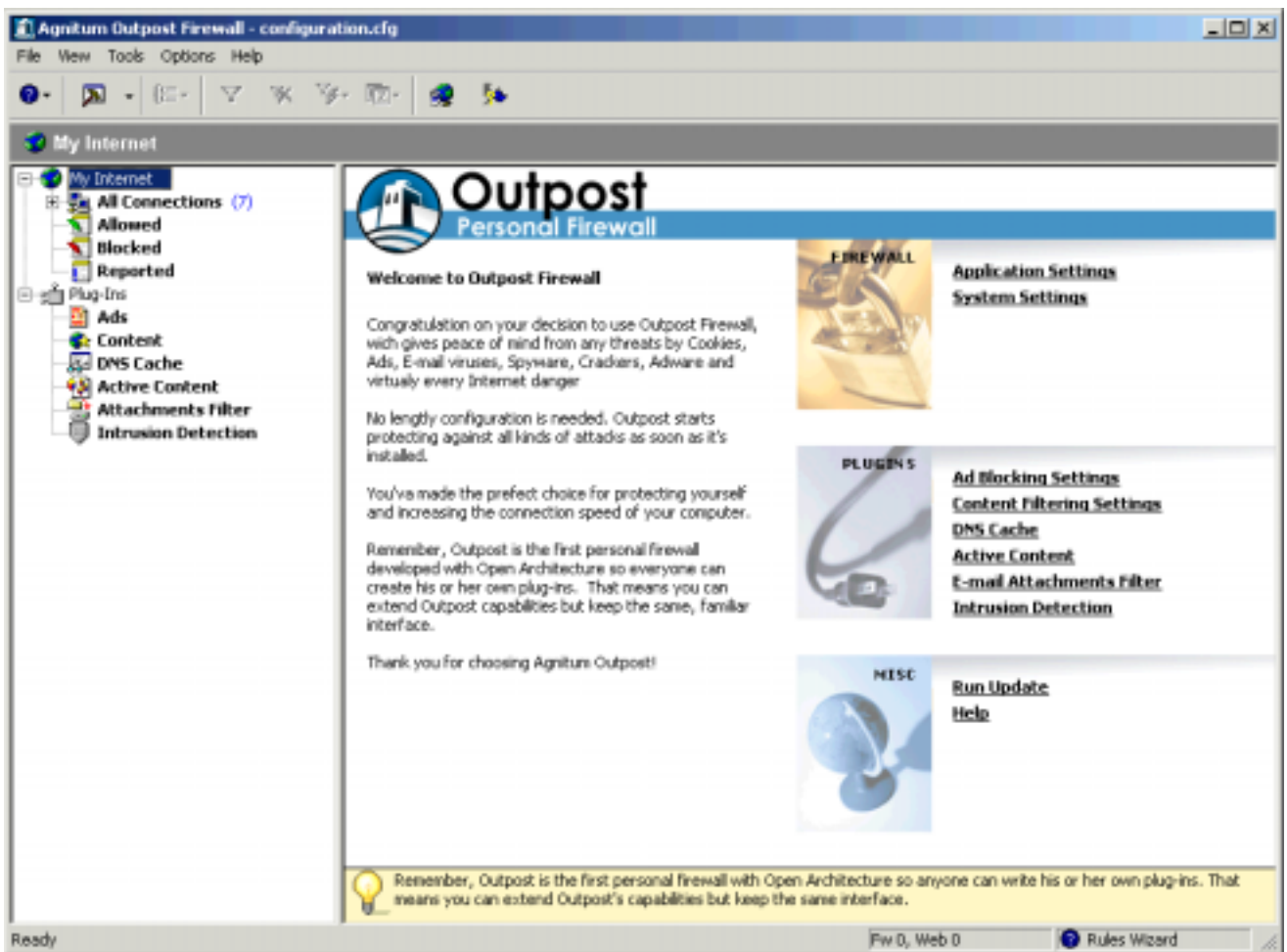
1. Right-click the  icon on the taskbar.
2. Select *Exit and Shutdown Outpost*.

Initial Options

Language

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

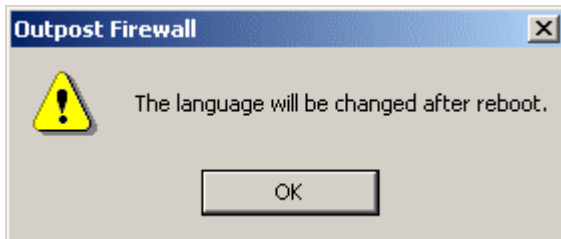
1. Double click the  icon on the taskbar. Outpost's main window is displayed and looks like this:



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 reboot your computer 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.

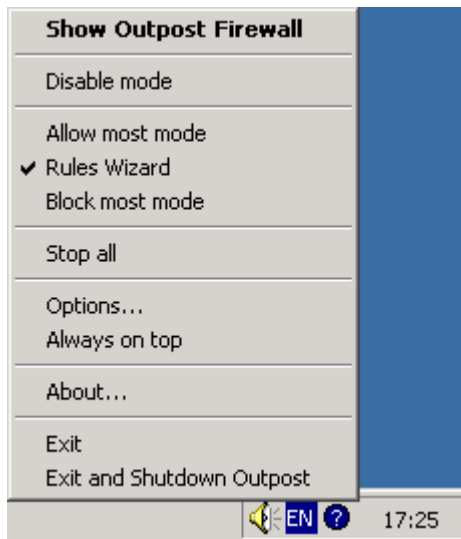
The operational modes are:

- 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**. The Outpost icon on the taskbar shows which mode is set.

To change the operational mode:

1. Right click on the taskbar icon (either , , ,  or )
2. The following menu appears. Select the operational mode by clicking on it.



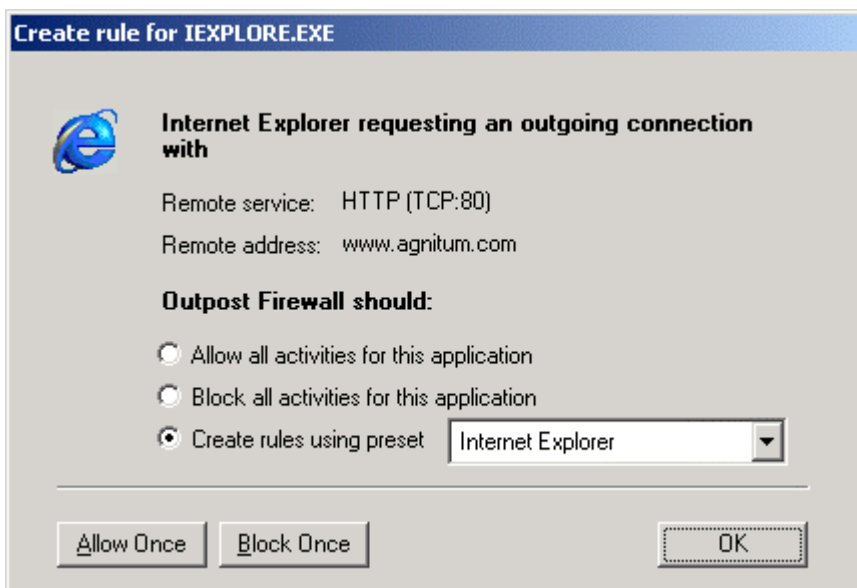
Rules Wizard

Rules Wizard is the operational mode that lets you decide each application's permissions to use the Internet. Outpost asks you whenever an 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 or not. 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 change or delete an app's rules very easily whenever you want.

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 you know should not to have network access. The application is included in the Blocked applications list. (See *Options* menu, *Applications* tab.)
- **Create rule using preset**—For applications you trust or distrust about the same as another app you have already set rules for. The application will be included in the Partially allowed applications list. (See *Options* menu, *Applications* tab.)
- **Allow Once**—For applications you are doubtful of. 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 you distrust but are uncertain of. 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's 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 *Help* menu then on *Automatically check for Update* 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.

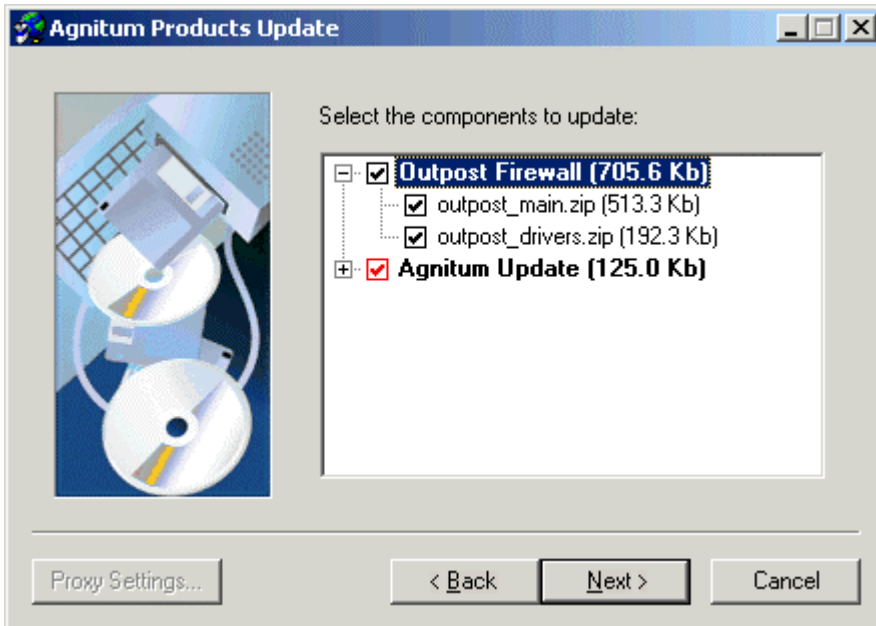
Whether checking manually or automatically, if there is an update, Outpost displays this dialog:



Automatic—all new modules are downloaded and installed. This is recommended for maximum protection.

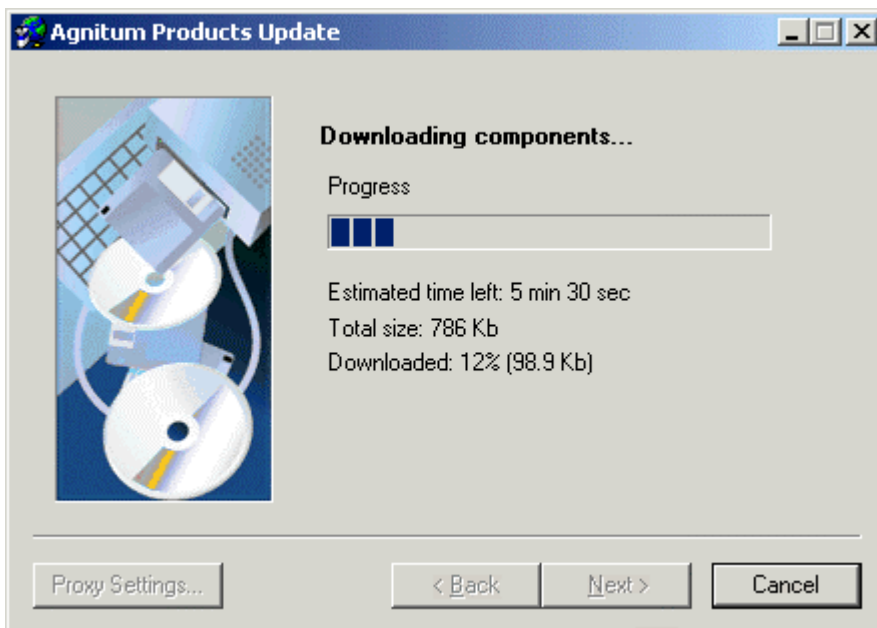
Custom—you can specify the modules you want updated.

If you select **Custom** before clicking the Next button you will see this dialog:

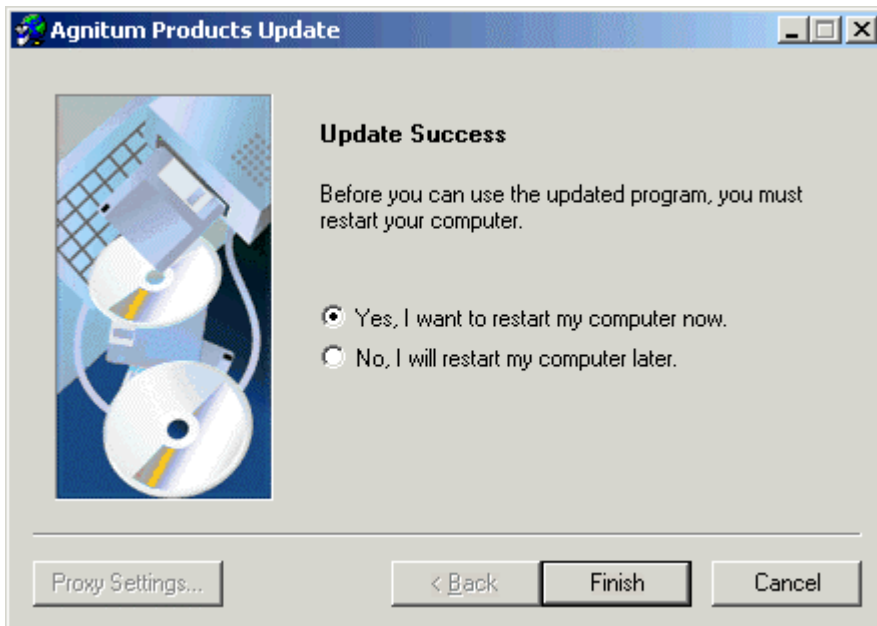


Check-marked items will be updated and unchecked items will not be. Clicking on the box toggles the check-mark on and off. This applies only to the black check boxes. A red check box shows the modules that will be downloaded with a checked item.

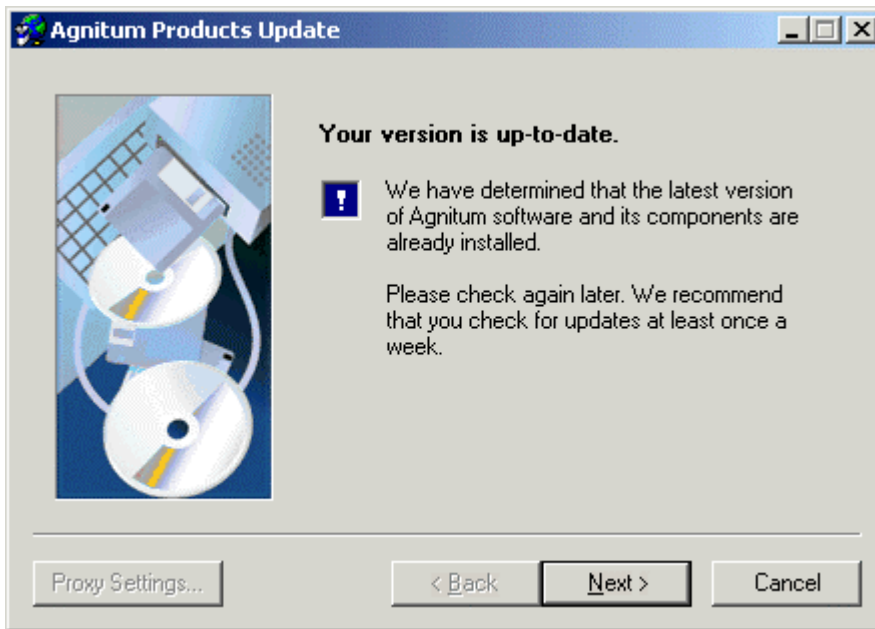
If updates are available the next screen is:



then:



If no updates are found or none are requested this is displayed:



Advanced Settings

Safeguarding Your Files

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.

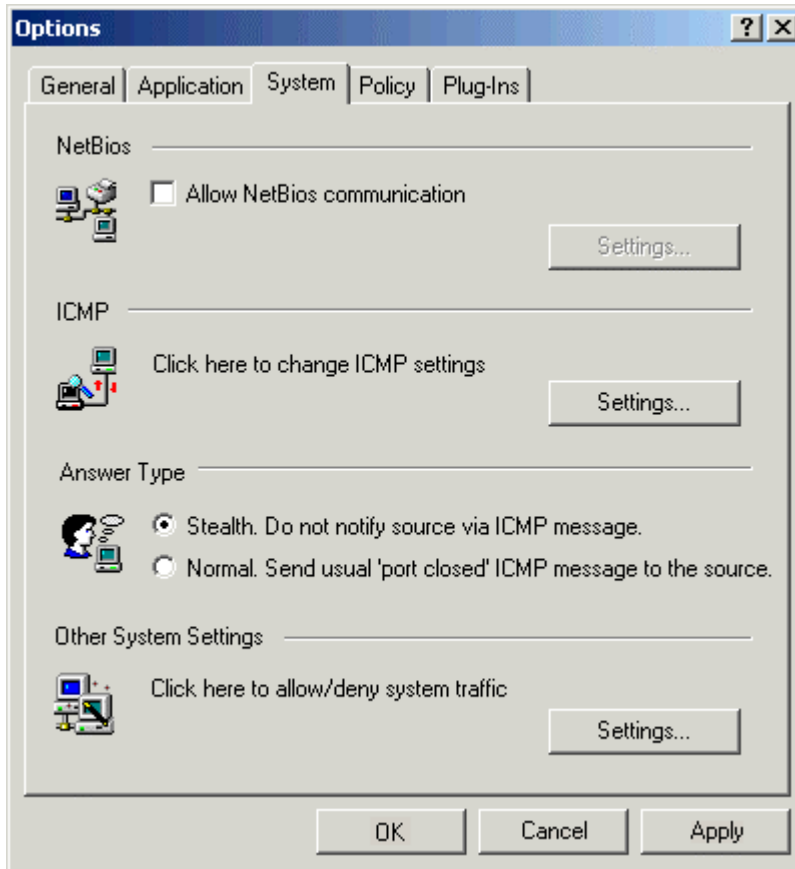
A Trojan on your computer can let a hacker view, copy or erase any folder and any file on your computer just as though he or she were sitting at your computer using its keyboard and mouse. Any file on your computer can also be sent to any e-mail address or posted on the Internet.

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

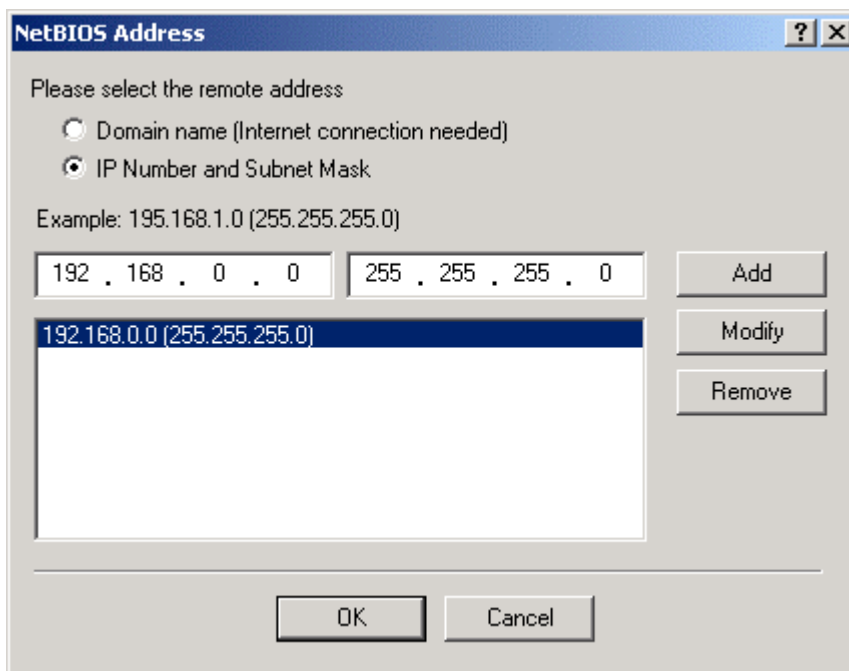
Outpost's settings for maximum protection from Trojans:

- **Rules Wizard** mode informs you of any program trying to send data from your computer.
- **Stop all** mode effectively disconnects your computer from the Internet, which can be set very easily whenever you are not working on the Internet.

- Make your computer invisible to hackers. Click on the *Options* menu, then on the *System* tab. Select **Stealth** in the *Answer Type* field.

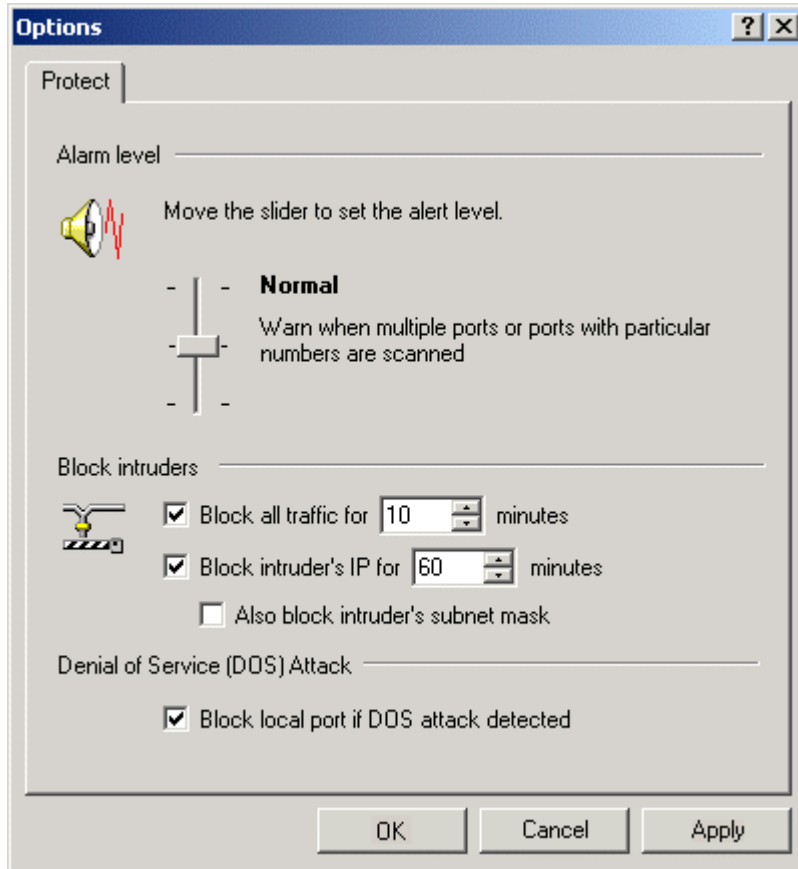


- Ensure **NetBios** is unchecked unless your computer is on a local network and needs to share its files. If you need to use **NetBios** check this field and click on its *Settings...* button to get the following dialog:



The IP address in the default list (shown in this picture) is the usual number and subnet mask of a local network. Outpost specifically trusts any items on this list. All other requests for a NetBios connection are blocked.

- In *Options*, click on the *Plug-Ins* tab and select *Intrusion Detection*. Click on the *Select* button then set the options as you see fit in this dialog:




Note: You can see the DNS or IP address to which a suspect program tries to send info by examining the logs. The categories of logs are listed in the left panel of Outpost's main window (Incoming, Outgoing, Allowed, Blocked and Reported). The Users Manual covers these logs in detail.

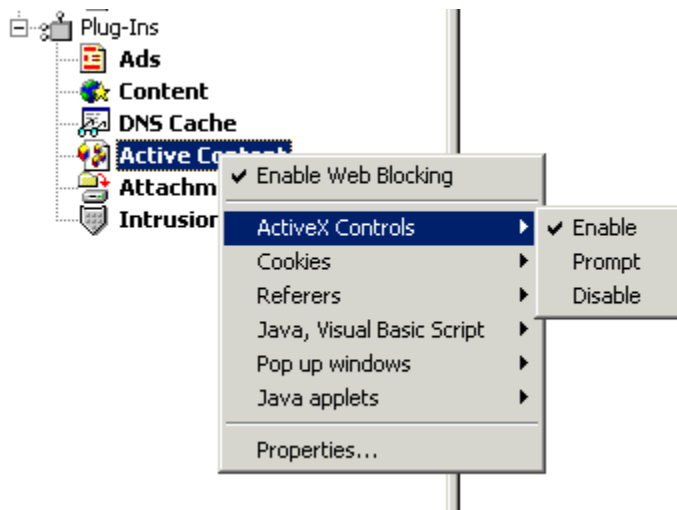
A Web Site's Hidden Programs

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.

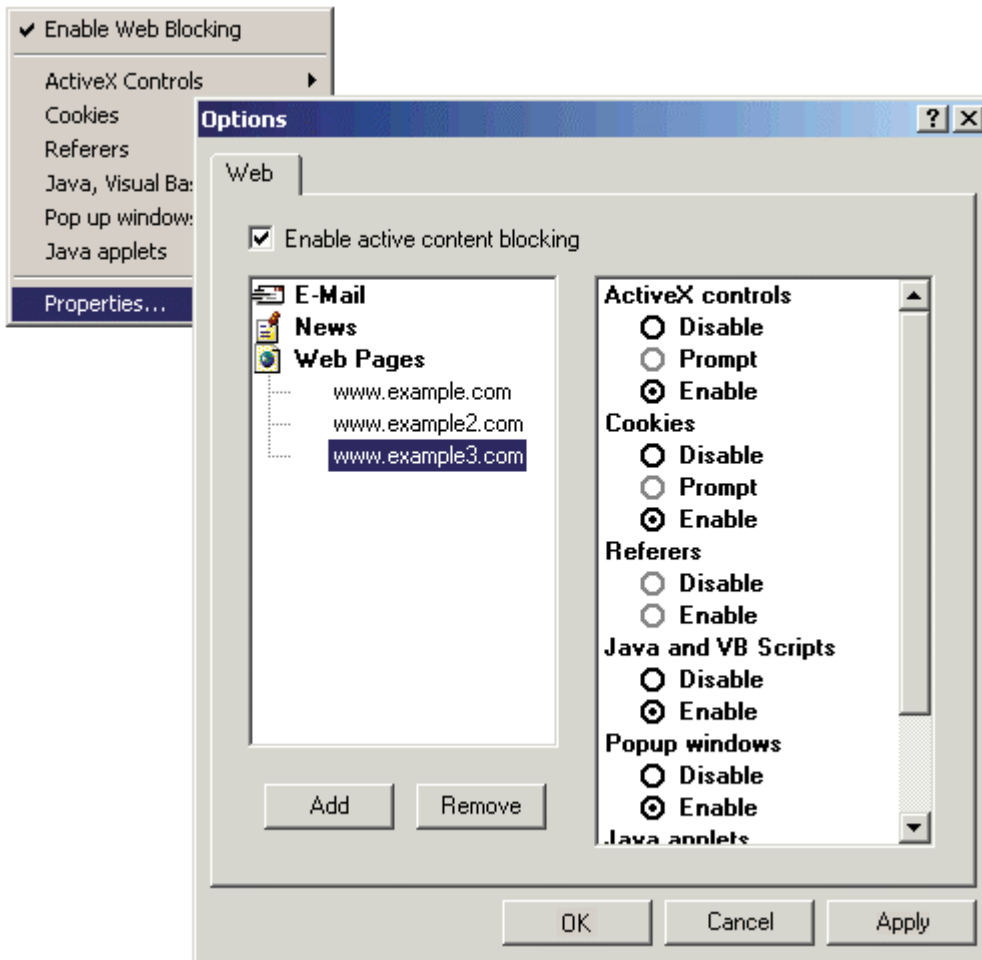
However, some hackers found ways to make embedded programs destructive so Outpost gives you the option of disabling each questionable component individually.

To do this:

1. Double-click the icon  on the taskbar to display Outpost's main window.
2. Right-click on *Active Content* to show its menu, which looks like this:

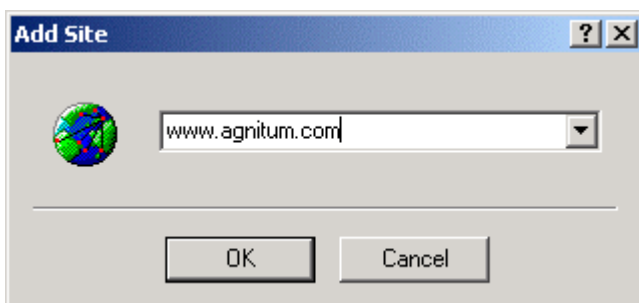


Clicking on *Properties* shows the same options organized differently:



The image shows three web sites listed under *Web Pages* (www.example.com, www.example2.com and www.example3.com). These sites can be configured individually by highlighting each one and setting its options.

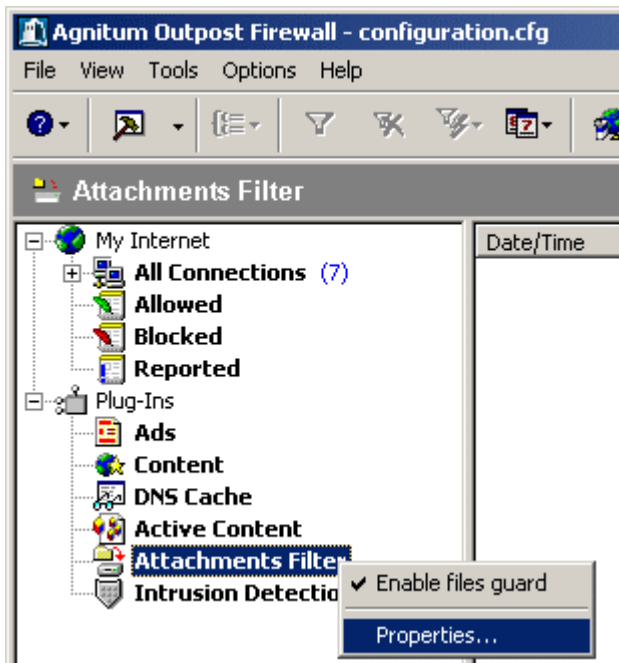
To add a new address to this list, click the Add button and enter the new address.



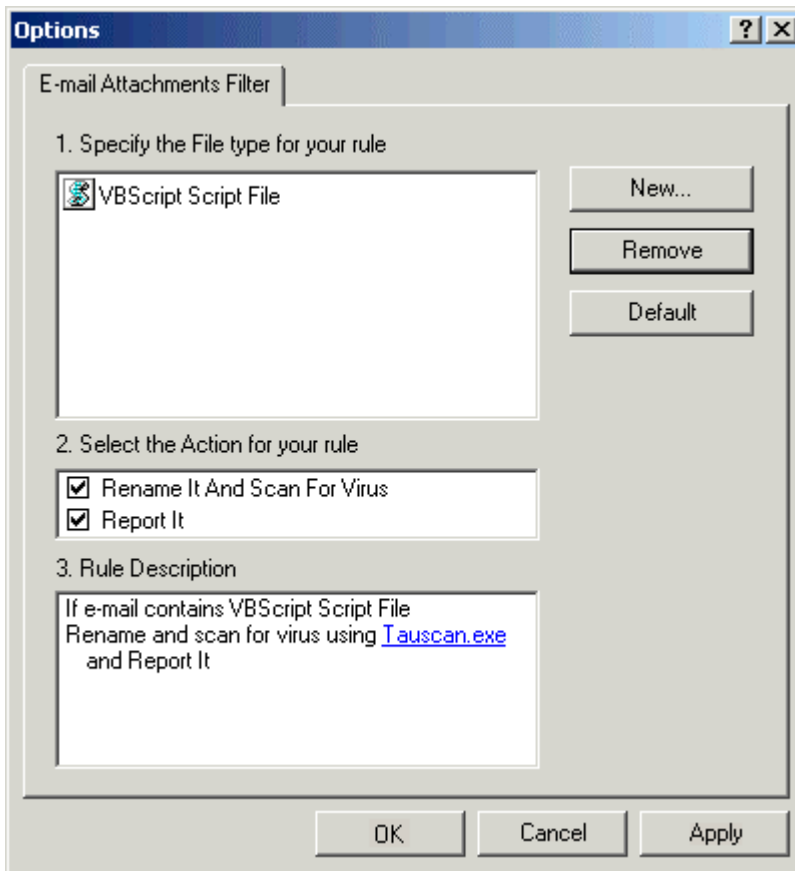
E-Mail Threats

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 how this is done.

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 a Trojan horse, a seemingly helpful program that opens 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 on *Attachments Filter* and selecting *Properties* like this:

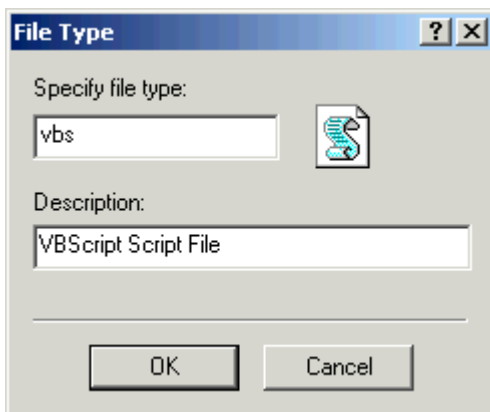


This gives you the following dialog:



In section 3 *Rule Description*, you can specify the anti-virus software to be used by clicking on its name (in this example, it is called **Tauscan.exe**).

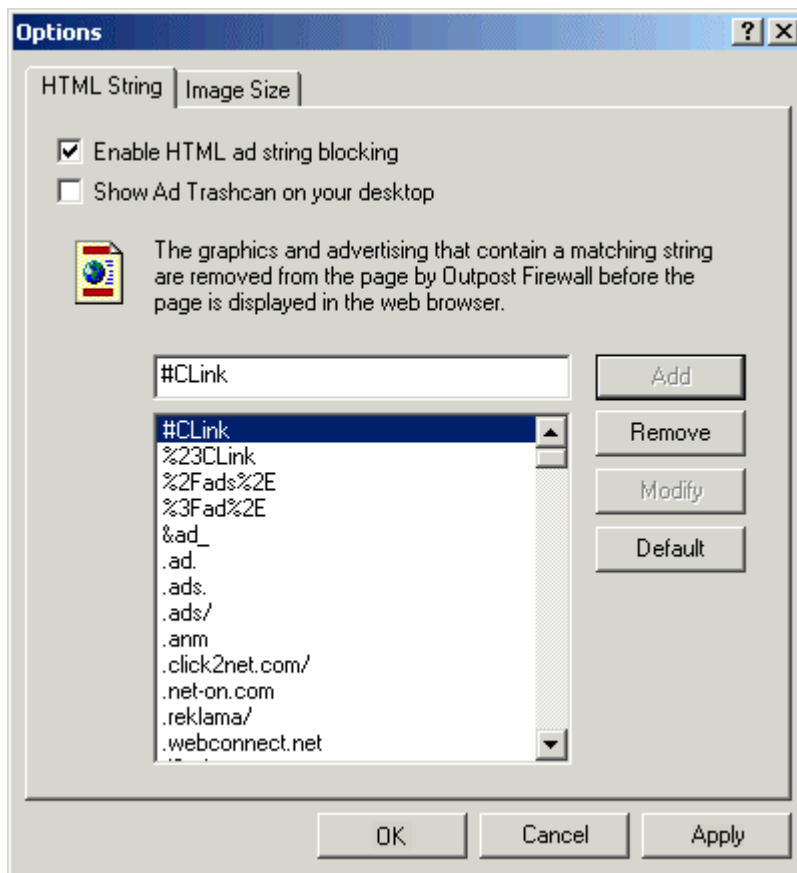
The *New* button lets you add file types to be inspected by Outpost and gives you this dialog:



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:

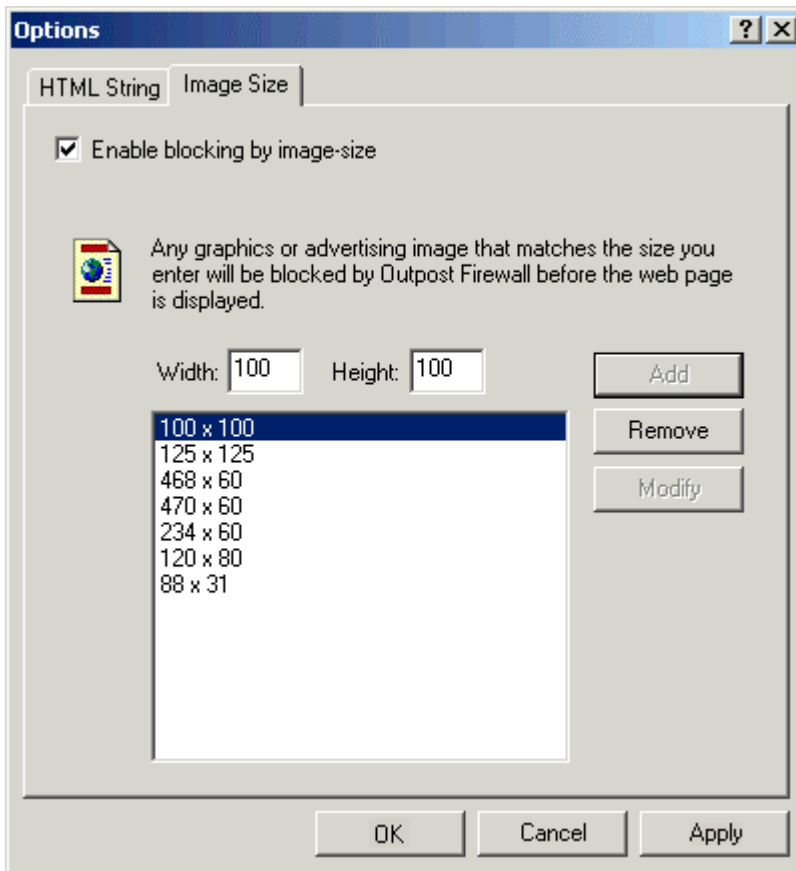


Ensure the **Enable HTML ad string blocking** checkbox is checked.

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 Size tab to get this dialog:



This dialog works similarly to the previous.

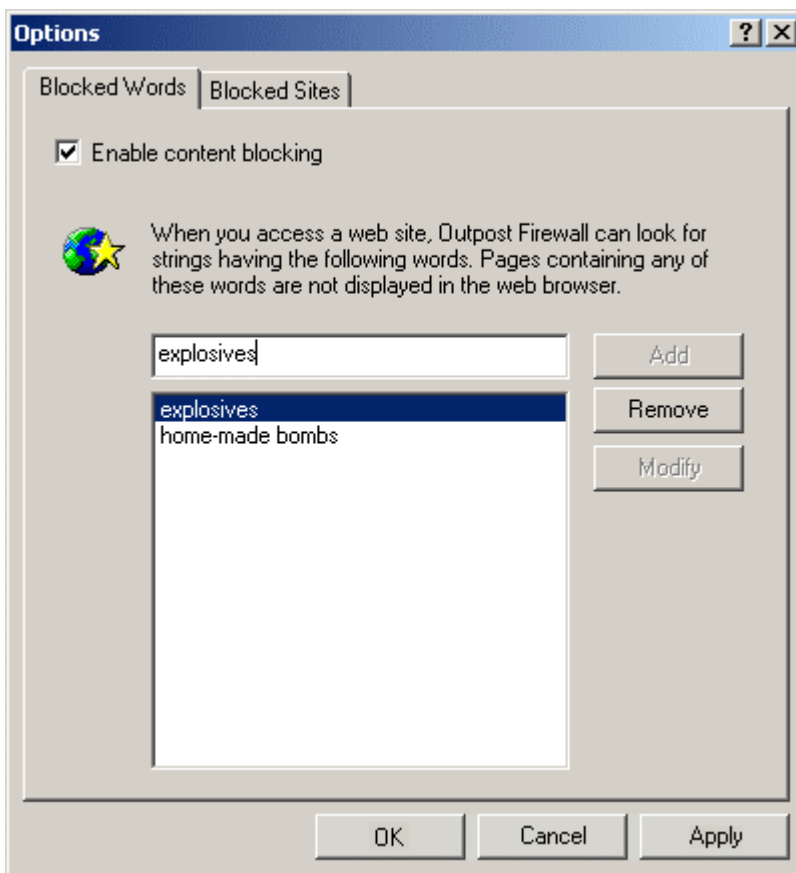
Note: Blocking ads by image size blocks the display of all images having the specified sizes **that are links** (i.e. within `<a` tags), whether they are linked to another site or a page within the web site.

Content Blocking

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

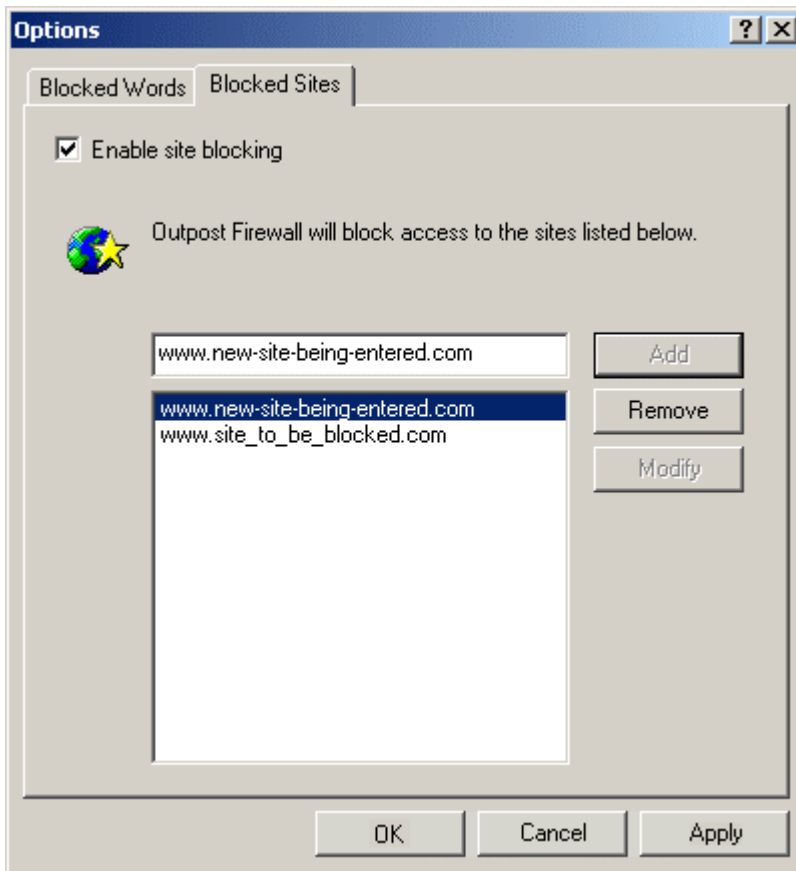
To have Outpost block objectionable content:

Right-click on **Content** in the left panel of Outpost's main window, then select Parameters to get this dialog:



This dialog works very similarly to the ad blocking dialogs.

To block specific web sites click on the **Blocked Sites** tab for this dialog:

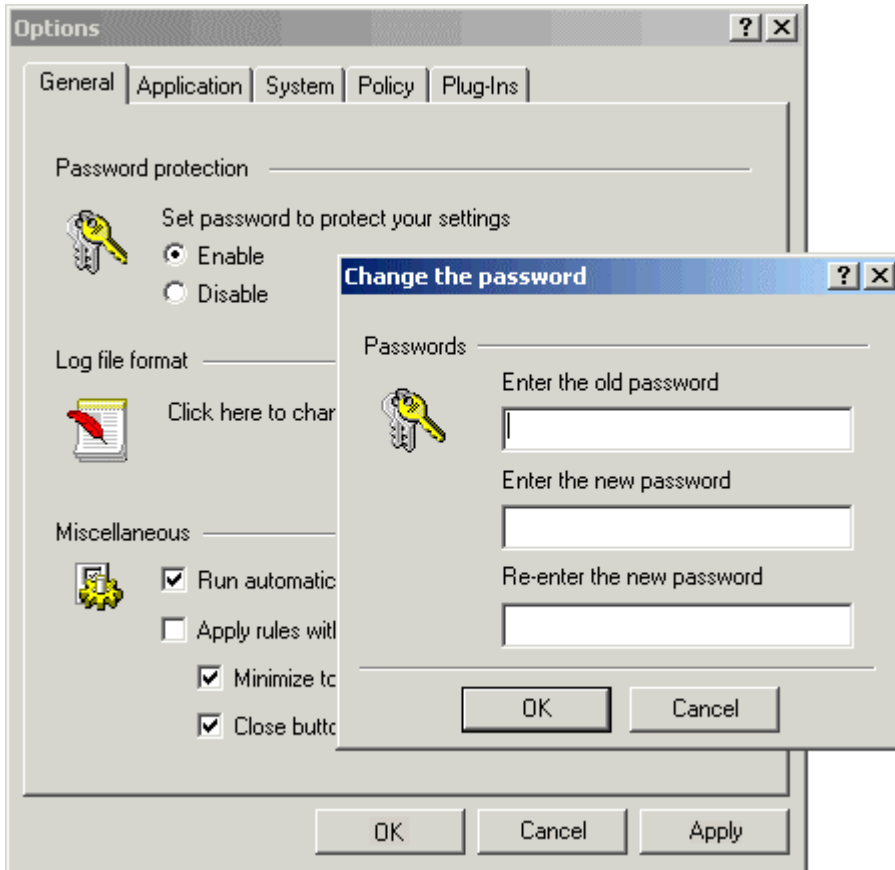


This dialog works similarly to the ad blocking dialogs.

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 General Options dialog as shown here:

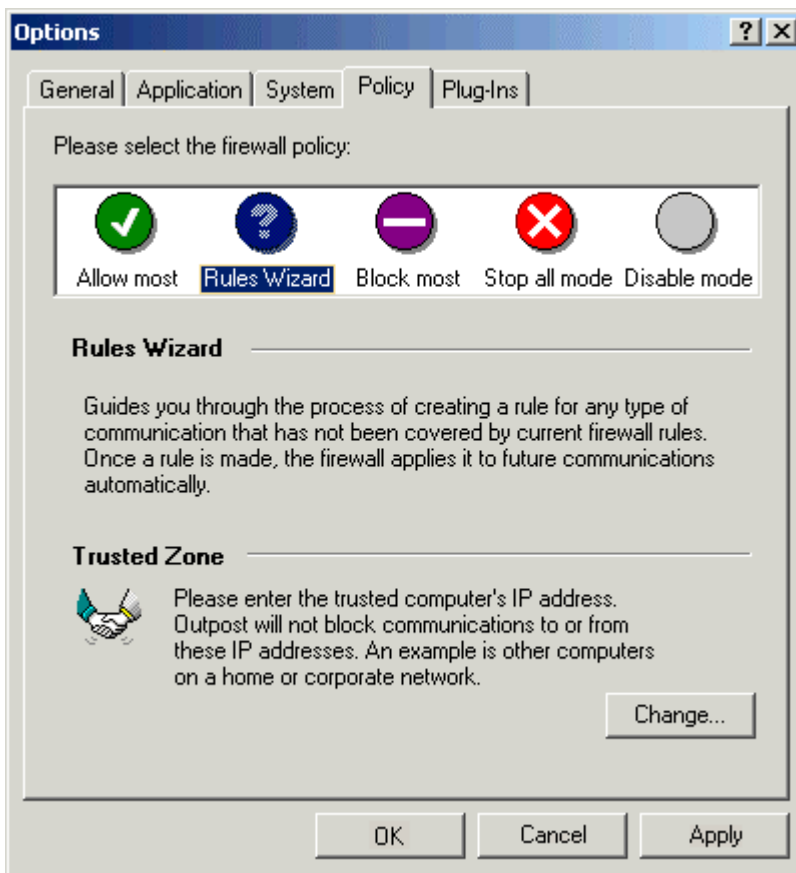


Skip the field **Enter the old password** if you have not already set one. This is used only if you are changing passwords.

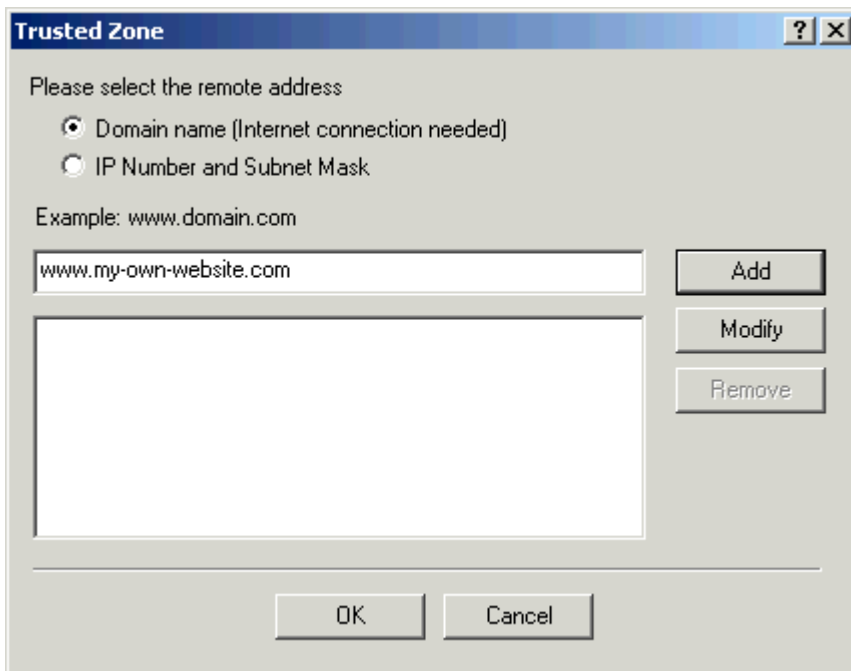
Trusted Zone

You can specify sites that you trust so Outpost does not block their traffic or ask you each time for your permission. Examples of trusted sites would be other computers on your local corporate or home network.

To specify a trusted site or computer click on *Options*, then on the *Policy* tab to get this dialog:



Click the **Change...** button to get the following dialog:



This dialog works similarly to the previous dialogs with the addition of the subnet mask.

For more in-depth information about Outpost, please see the User Manual.