User Guide

Reference

Outpost Security Suite 2007

Personal Security Software
from
Agnitum

Abstract

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

For an entry-level guide, please see the Quick Start Guide.

Table of Contents

Welcome

This User Guide is arranged in two parts. The first part is for all users, but the second part is intended only for those users who are technically advanced.

Part 1: For All Users

1 Getting Started

1.1 Starting Outpost Security Suite

Once installed, the **Outpost Security Suite** starts automatically when Windows is loaded. Thus, **Outpost Security Suite** starts protecting your computer immediately before other programs can compromise your system.

When **Outpost Security Suite** starts, its icon is placed in the system tray, on the right-hand end of the Windows task bar.

If, for some reason, **Outpost Security Suite** does not start when Windows loads, you can start it by following these steps:

1. Click the Windows **Start** button and select **Programs**.
2. Select **Agnitum**.
3. Select **Outpost Security Suite**.
4. Select **Outpost Security Suite**.

When **Outpost Security Suite** is running its icon is displayed in the system tray. If you do not see the **Outpost Security Suite** icon in the system tray, then you know that **Outpost Security Suite** is not protecting your computer unless you specifically set it up to run in background mode. For more info please refer to the 3.2 Initial Settings chapter.

1.2 Stopping Outpost Security Suite

Closing **Outpost Security Suite's** main window does not shut down the product. Its icon remains in the system tray.

There are two ways to shut down **Outpost Security Suite**:

- Right-click its icon in the system tray to display the shortcut menu. Select **Exit**.
- You can also shut down **Outpost Security Suite** when its main window is displayed by going to the **File** menu and select **Exit**.

Both ways close the interface and stop the firewall so **Outpost Security Suite** is no longer protecting your system.

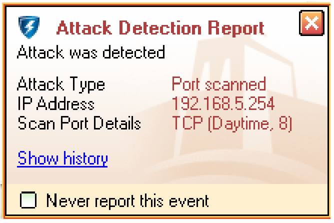
When Outpost Security Suite is shut down its icon disappears from the system tray indicating that the firewall is no longer protecting your computer.

1.3 Outpost Security Suite Alerts

Outpost Security Suite displays alerts to notify the user of specific events and keep the user aware of the activities performed by **Outpost Security Suite**.

Alerts are displayed in popup boxes that automatically close in ten seconds. To keep a lengthy alert from closing so you can read it fully, simply click anywhere in the pop-up box.

The example of alert displayed by **Outpost Security Suite**:



Attack Detection Report

Attack was detected

Attack Type	Port scanned
IP Address	192.168.5.254
Scan Port Details	TCP (Daytime, 8)

Show history

☐ Never report this event

In this case, Outpost Security Suite has detected and blocked an attack against your system. The alert message displays the attack details. Click **Show history** to see the full list of all attack reports of this same type.

Note: This alert is displayed only when the **Report detected attacks** option is selected in the Attack Detection plug-in settings dialog box.

Outpost Security Suite automatically downloads the latest news and plug-ins announcements from Agnitum web site and displays them when you click **My Internet** or **Plug-Ins** in the left panel tree in the main window.

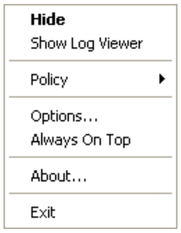
Tip: To disable this feature, right-click **My Internet** or **Plug-Ins** and clear **Download Agnitum News** and/or **Download Plug-Ins Information**.

2 An Orientation

2.1 The System Tray Icon

The system tray is the right most part of the Windows taskbar. The white tower on the blue shield is Outpost Security Suite's icon: . This icon is one of the primary ways you can access Outpost Security Suite's many controls, settings and logs.

When you right-click the **Outpost Security Suite** icon you get its shortcut menu:



The following items are available on this menu:

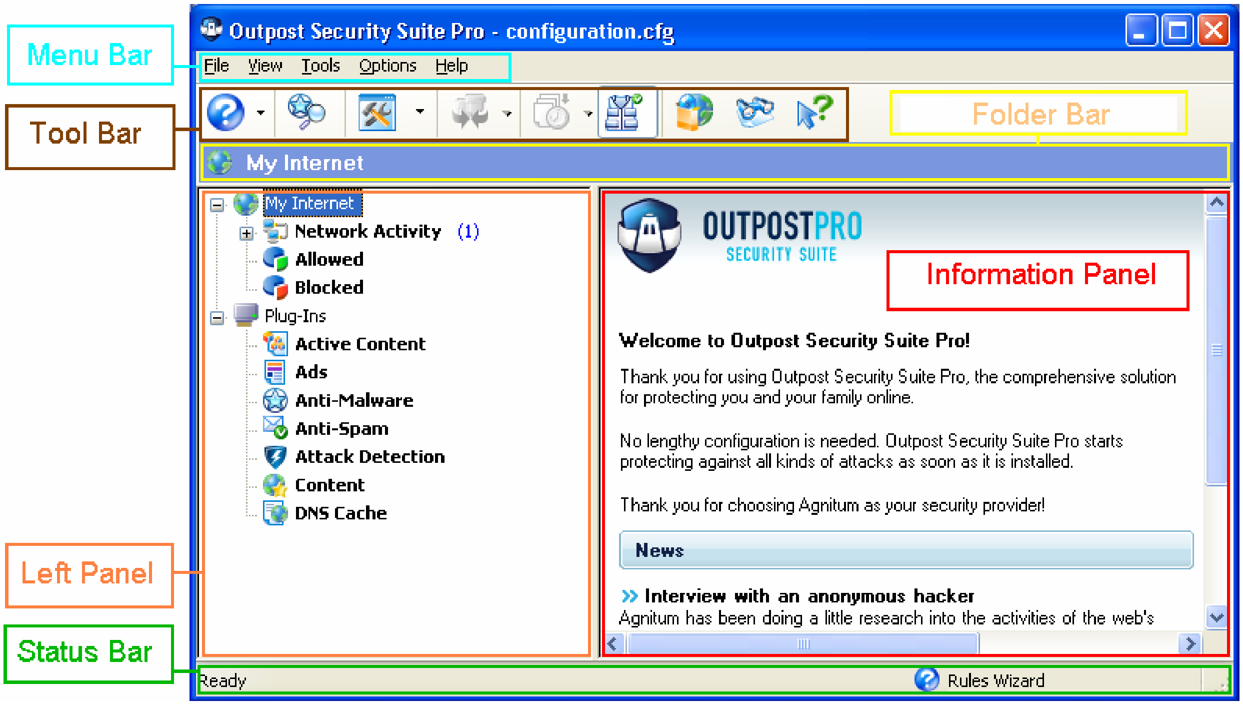
- **Show—**displays **Outpost Security Suite's** main window.
- **Show Log Viewer**—displays **Outpost Log Viewer.**
- **Policy—**opens a sub-menu where you can change **Outpost Security Suite's** policy to the following: **Disable mode**, **Allow most mode**, **Rules Wizard mode**, **Block most mode** or **Stop all mode**.
- **Options—**displays the **Options** dialog window.
- **Always on top—**when selected, keeps **Outpost Security Suite's** current window on top of all other windows.
- **About—**shows the current version of **Outpost Security Suite** and lists each module in the package and their individual versions.
- **Exit—**closes the GUI and stops the suite so **Outpost Security Suite** is no longer protecting your system.

2.2 Outpost Security Suite's Main Window

The **Outpost Security Suite** main window is used to monitor the network operations of the computer and to modify the settings.To display **Outpost Security Suite's** main window:

1. Right-click the **Outpost Security Suite** system tray icon.
2. Select **Show** on the shortcut menu.

This is what the **Outpost Security Suite** main window looks like right after **Outpost Security Suite** is installed:



Welcome to Outpost Security Suite Pro!

Thank you for using Outpost Security Suite Pro, the comprehensive solution for protecting you and your family online.

No lengthy configuration is needed. Outpost Security Suite Pro starts protecting against all kinds of attacks as soon as it is installed.

Thank you for choosing Agnitum as your security provider!

News

» Interview with an anonymous hacker
Agnitum has been doing a little research into the activities of the web's

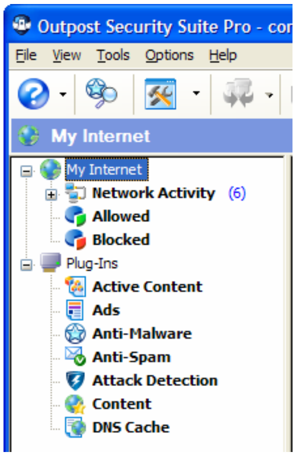
The main window contains:

- **Outpost Security Suite's** menu
- Toolbar
- Folder bar
- Left panel
- Information panel
- Status bar.

2.3 The Panels

The left panel and information panel are similar to the left and right panels of Windows Explorer. The left panel is a listing of the components secured by **Outpost Security Suite** on your computer and the information panel gives specific data about any component highlighted in the left panel.

Here is the left panel:



Under **My Internet** are the items:

- **Network Activity**—shows every application and protocol that currently has an active connection to the Internet or LAN as well as other network activity.
- **Open Ports—**shows your system's open ports.
- **Allowed**—shows the event log stats for all the applications and connections that **Outpost Security Suite** allowed. You can view the stats filtered for the current session, current day or all times.
- **Blocked**—shows the event log stats for all the applications and connections that **Outpost Security Suite** blocked. You can view the stats filtered for the current session, current day or all times.
- **Reported**—is the event log of all the attempts by applications and connections to access the Internet or LAN that you specified **Outpost Security Suite** to report to you.

Although the details of the logs are intended for advanced users, the above items are important when you need to see the stats on established connections or bytes sent and received. To view the logs in more detail, advanced users should press the **Show Detailed Log** button located on the information panel of Allowed, Blocked and Reported items (please refer to 6 The Outpost Log System chapter for more information). You can also use the detailed statistics to make certain that **Outpost Security Suite** is correctly configured and functioning properly.

The **Outpost Security Suite** setup package that you downloaded from Agnitum web site contains some additional plug-ins. Plug-ins are independent from the primary **Outpost Security Suite** engine and you may install or uninstall any or all of them. You can even get third-party plug-ins from other developers and web sites. The second part of the listing of the left panel shows the plug-ins that are installed.

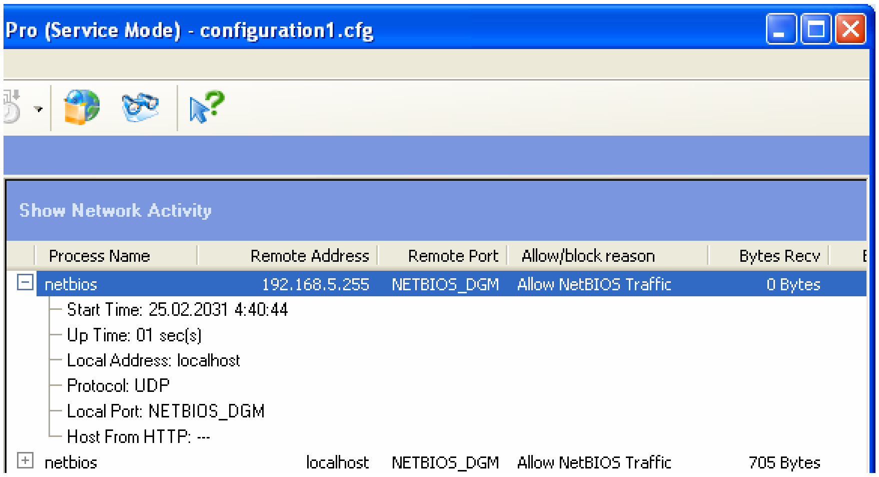
Each plug-in has its own icon in the left panel and the log of its activity is displayed in the information panel. When **Outpost Security Suite** is first installed the **Plug-Ins** list contains the following modules:

- **Ads**—displays the events log of all the ads that were blocked.
- **Content**—displays the events log of all the web sites or pages that were blocked by this plug-in and the reason why.
- **DNS Cache**—displays the events log of the web addresses cached by **Outpost Security Suite** to speed up your Internet connection to those sites.
- **Active Content**—displays the events log of the sites that had some of its active content blocked based on the settings for Java applets, VBScript, ActiveX, and other active content elements.
- **Anti-Spam**—shows the events log of received junk e-mail.
- **Attack Detection**—shows the events log of any suspected attacks on your computer from the Internet, the ports involved and where the attacks are from.
- **Anti-Malware**—shows the events log of malware objects detected in your system.

As with Windows Explorer, any line that starts with a plus sign (+) can be expanded to show each of its subcomponents. In the picture above, the **Network Activity** line can be expanded by clicking on the plus sign at the start of that line.

Any line starting with a minus sign (-) shows that the line has already been expanded. By clicking on the minus sign, all of its subcomponents can be hidden so only the type of component is displayed to conserve screen space.

Here is an example of the information panel showing some of the many types of data it displays:



Pro (Service Mode) - configuration1.cfg

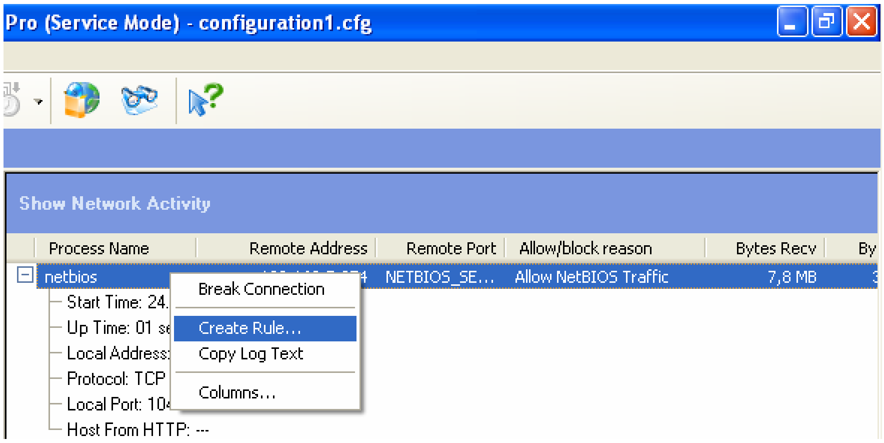
Show Network Activity

```
   Process Name          Remote Address   Remote Port   Allow/block reason        Bytes Recv   E
⊟ netbios                 192.168.5.255   NETBIOS_DGM   Allow NetBIOS Traffic       0 Bytes
    ├ Start Time: 25.02.2031 4:40:44
    ├ Up Time: 01 sec(s)
    ├ Local Address: localhost
    ├ Protocol: UDP
    ├ Local Port: NETBIOS_DGM
    └ Host From HTTP: ---
⊞ netbios                     localhost   NETBIOS_DGM   Allow NetBIOS Traffic     705 Bytes
```

The line which has a minus sign by its side is expanded to show its individual data. To hide this extra data, click the category's minus sign. A line without a plus or minus sign preceding has no extra data to be shown.

For advanced information about customizing the information panel, see the Columns section of the **Appendix A**.

As with most elements of **Outpost Security Suite**, a right-click in the information panel opens a shortcut menu. In the picture below, the menu is pertinent to the highlighted line. If no line was highlighted and the right-click was over some of the white space below the lines, then all the menu items would not be applicable and so would be grayed out.



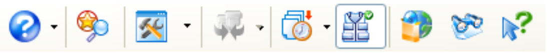
Process Name	Remote Address	Remote Port	Allow/block reason	Bytes Recv	By
⊟ netbios	…4	NETBIOS_SE…	Allow NetBIOS Traffic	7,8 MB	
Start Time: 24.					
Up Time: 01 se					
Local Address:					
Protocol: TCP					
Local Port: 10					
Host From HTTP: ---					

The menu shown in the above picture is for displaying the data in the information panel in a way that is most useful to you. This is mainly for professionals like system administrators who need to rapidly track down some particular data. Although **Outpost Security Suite** is easy enough for a home computer user, it is also very sophisticated to meet the needs of advanced users.

The choices in the menus shown above are self-explanatory to those users who would need to use them. **Outpost Security Suite** makes extensive use of shortcut menus for all of its different items, categories, panels, and icons. A little experimenting will help you discover all of them and is far more instructive than reading detailed descriptions of each item.

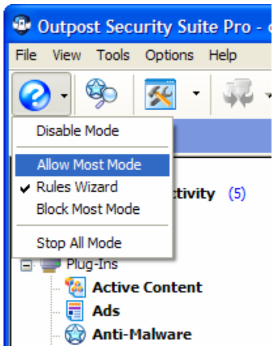
2.4 The Toolbar

The toolbar is close to the top of the main window and looks like this:



You can see what each button does by holding your cursor over it for a second or so.

The icon in the left end of the toolbar shows **Outpost Security Suite's** current policy. Clicking on this icon gives a menu you can use to quickly change usage modes. The menu looks like this:



Only some of the buttons are visible (active) at any one time, depending on what is highlighted in the left panel or the information panel.

The buttons are simply an easy and direct path to their functions rather than having to go through several different menus or dialog windows to access these same functions.

Outpost Security Suite's Toolbar Buttons

Button	Function	Corresponding Menu Path
	Changes **Outpost Security Suite's** policy	**Options > Policy**
	Starts malware system scan.	**Tools > Run Malware System Scan**
	Accesses the Options dialog window	**Options**
	Changes the listed item grouping	**View > Group By**
	Narrows a log listing to events within a specified time	**View > Filter By Time**
	Enables/disables Self-protection mode.	**Tools > Enable Self Protection**
	Checks for an update of **Outpost Security Suite**'s plug-ins or components	**Tools > Agnitum Update**
	Opens **Outpost Log Viewer** that displays the logs	**Tools > Log Viewer**
	Displays **Outpost Security Suite's** context help	**Help > Context Help**

3 Setting up Outpost Security Suite

3.1 Basic Information

A firewall for your computer is like the lock on a door of your home. In most cities, we usually lock the front door of our homes when we leave. This is not because the majority of people are criminals or because we cannot trust our neighbors to mind their own business. We generally lock our doors to prevent criminal types from snooping, stealing or doing damage.

The Internet is similar. Most web sites are unobtrusive and benign. Only a small percentage holds any threat to our privacy. However, because there are such a huge number of Internet users, even a small percentage of them with an impulse to vandalize adds up to a very significant number of people. For this reason, leaving your computer unprotected is just not prudent.

Outpost Security Suite is engineered to detect a suspicious connection. It is recommended that you keep the firewall in **Rules Wizard** mode for several days use. **Rules Wizard** is the easiest for you to use if you are unfamiliar with how firewalls work.

NOTE: If you have any doubt or confusion about changing any default setting, it is recommended that you DO NOT MAKE THE CHANGE. Even if you do understand the change, it is advisable to save or record the setting before changing it.

When **Outpost** alerts you of a suspicious connection request from an application on your computer or from the Internet, it gives you some information about the request, such as the DNS or IP address of the remote computer, the application making the request and other data to help you decide if you want to allow the connection or not. If in doubt, simply disallow the connection **this one time**. See what happens. If you are prevented from doing something you wanted to do, then just try doing it again and this time **allow** the connection when prompted. In this way, you can learn what your applications are doing and which ones you need to be careful of or even uninstall completely from your system. It will also alert you to the presence of a Trojan horse.

Note: A good rule of thumb when using **Outpost** is to keep the settings **Outpost** suggests if you do not have a particular reason and the knowledge to change them.

In **Outpost Security Suite** an access setting is basically a rule that you set regarding how much of your information you want to let other computers access or how much information you want to allow other computers to send to yours.

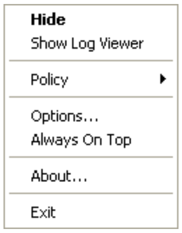
Outpost Security Suite uses various security settings to keep your computer protected from unwanted access from other computers on the Internet or any type of network connection. It also restricts the flow of information coming into your computer as you see fit. You might set a rule about file sharing, for example, so that your computer shares your files only with other computers you trust on your local network. A common use for a firewall is to restrict the amount of information your computer gives out while it is connected to the Internet.

3.2 Initial Settings

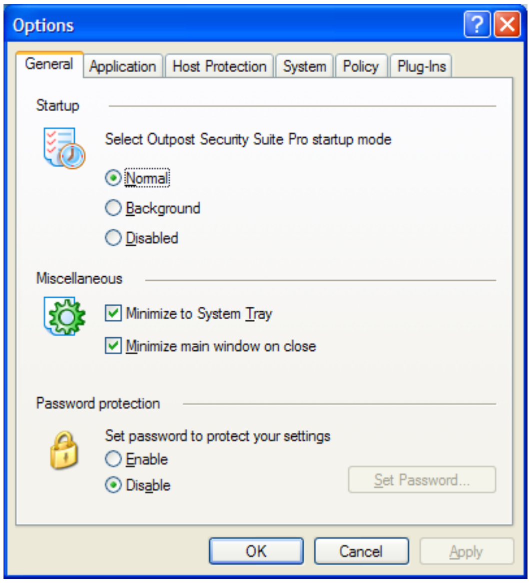
Outpost Security Suite is ready for operation as soon as it is installed. Its default settings are more than adequate for most purposes and are recommended until you become fully acquainted with how **Outpost Security Suite** operates. Once you are familiarized, you can customize **Outpost Security Suite** in many ways to best suit your particular needs.

This section gives a brief overview on how to customize the system. You can change these settings at any time.

To display the **Outpost Security Suite** settings dialog window, right-click the **Outpost Security Suite** system tray icon and select **Options** from the shortcut menu:



The settings dialog looks like this:



Startup

Select Outpost Security Suite Pro startup mode

● Normal
○ Background
○ Disabled

Miscellaneous

☑ Minimize to System Tray
☑ Minimize main window on close

Password protection

Set password to protect your settings

○ Enable
● Disable

The first section is **Startup**. This lets you choose the startup mode for **Outpost Security Suite**. The default startup mode is **Normal,** which loads **Outpost Security Suite** automatically at boot-up and displays its icon in the system tray. Select **Background** if you want **Outpost Security Suite** to run in invisible mode, without its system tray icon or any of its dialog windows. This option is provided for two reasons: to save system resources and for a parent or systems administrator to block unwanted traffic or content in a way that's completely hidden from a user. If you do not want Outpost Security Suite to run automatically at startup, select **Disabled**.

The **Miscellaneous** area of the dialog is where you can select **Minimize to System Tray** to not have a button placed on the task bar for **Outpost Security Suite's** main window whenever it is minimized. Instead of this, to see **Outpost Security Suite's** main window, simply double-click **Outpost Security Suite's** system tray icon or right-click it and select **Show**.

If **Minimize main window on close** is selected, then whenever you click the close button ☒ only **Outpost Security Suite's** main window will be closed, not the firewall. In this case, to shutdown **Outpost Security Suite**, right-click **Outpost Security Suite's** system tray icon and select **Exit**.

The **Password protection** section lets you select to have your **Outpost Security Suite** settings protected by password so only you can change its configuration.

3.3 Selecting a Policy

One of the most useful and important features of **Outpost Security Suite** is its usage modes. A usage mode is the basic attitude you want **Outpost Security Suite** to have in doing its job of policing your computer's access to and by the Internet or any other network your computer may be connected to. The usage mode of **Block most**, for example, gives **Outpost Security Suite** a particularly strict attitude but **Allow most** makes **Outpost Security Suite** very trusting.

Here are the different usage modes:

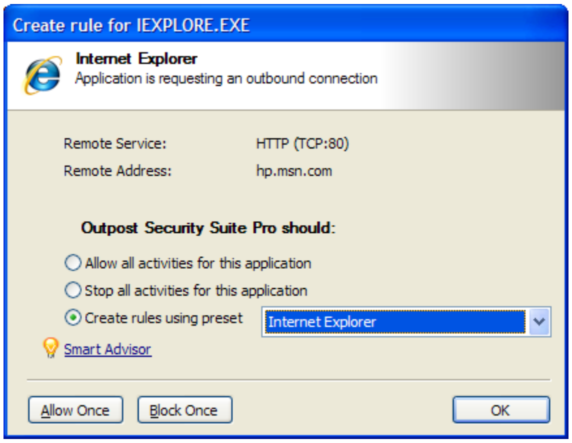
Icon	**Mode**	**Description**
⊗	Stop all	All network connections are blocked.
⊖	Block most	All network connections are blocked except those you explicitly allowed.
?	Rules Wizard	The first time each application is run, allows you to determine how an application will interact with the network.
✓	Allow most	All network connections are allowed except those you explicitly blocked.
○	Disable	All network connections are allowed.

When **Outpost Security Suite** is installed, the default mode is **Rules Wizard** mode. This mode helps you decide whether an application should be allowed a network connection.

Rules Wizard facilitates the specifying of applicable network parameters for each type of application.

Although during the installation process **Outpost Security Suite** creates the rules for applications already installed on your system, it might miss a few uncommon programs so at this point **Rules Wizard** mode makes your life a little easier. Instead of having to create a new and often complex rule each time a new application is run, **Rules Wizard** does the work for you by basing its presets on all well-known applications. **Rules Wizard** even recommends the best selection for you. Unless you **know** of a better choice, simply okay **Outpost's** recommendation.

Here is the **Rules Wizard** dialog window that pops up whenever a new application requests a network connection:



Create rule for IEXPLORE.EXE

Internet Explorer
Application is requesting an outbound connection

Remote Service: HTTP (TCP:80)
Remote Address: hp.msn.com

Outpost Security Suite Pro should:

○ Allow all activities for this application
○ Stop all activities for this application
● Create rules using preset Internet Explorer

Outpost Security Suite has a database of the most commonly used applications. Our engineers programmed the optimum settings for each type of application so the decisions you have to make are very few.

The **Outpost Security Suite** system groups applications into three groups.

- **Blocked—**distrusted applications for which all connections are blocked.
- **Partially allowed—**applications granted limited network access by having their protocols, ports and directions specified by policies (rules).
- **Trusted—**applications for which all connection requests are allowed.

In the picture of the dialog window above, you can see what application is requesting an outgoing connection, "Internet Explorer", what manner of access is being attempted, the basic parameters of the connection and the choices you can make regarding the request.

The choices you can make for an application in **Rules Wizard** mode are as follows:

Choice	**Purpose**	**Result**
Allow all activities for this application	For applications you trust completely.	All network requests by this application are allowed and the application is given the status Trusted application.
Stop all activities for this application	For applications that should not be allowed network access	All network activities for this application are disabled. The application is given the status Blocked application.
Create rules using preset	Restrict access for applications that interfere with network under specific protocols, via specific ports, etc.	Creates a rule for the application that limits network access to specific ports and protocols using presets designed by our engineers that are optimum for most purposes. This application will be included in the Partially allowed applications list.
Allow once	For applications that you are doubtful of but want to see what they do with the connection.	Data from specified local port to specified remote port and address is allowed during this single communication. The next time this application tries to establish a network connection, this same dialog window appears. No rule is created for the application.
Block once	For applications that you do not trust but do not want to block totally.	Data from specified local port to specified remote port and address is blocked during this single communication. The next attempt by this application to establish a network connection results in this same dialog window. No rule is created for the application.

Outpost Security Suite will detect most of the applications that regularly access the network after working a day or so in **Rules Wizard** mode. Once **Outpost Security Suite** has registered most of your applications, you can switch to **Block most** mode.

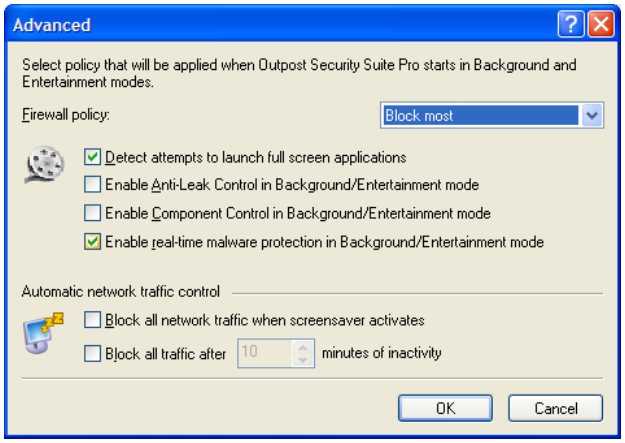
You can also create your own rule for an application rather than select one of the presets. To create a rule, click the down arrow at the right side of the **Create rules using preset** pull down. Select **Other** from the drop-down list and click **OK**. This brings up the **Rules** dialog where you can create any rule for this application.

Note: In the case when some application requests the connection to the server that has several IP addresses, Outpost Security Suite automatically detects all server addresses and configures corresponding rules for *all* server IP addresses according to the action you specify.

Note: Outpost Security Suite can perform on-the-fly malware scan of the processes requiring network access for which no rules exist and display the result in the Rules Wizard window header. For details, see the Anti-Malware section.

Rules Wizard is not supported when **Outpost Security Suite** is run in background mode as that mode is designed to run without user interaction.

If you select **Rules Wizard** and then try to run in background mode, you will need to choose another policy for **Outpost Security Suite** to use instead of **Rules Wizard**. Click on the **Policy** tab in the **Options** dialog box, then click on the **Advanced** button and select the policy in the displayed dialog:



Advanced

Select policy that will be applied when Outpost Security Suite Pro starts in Background and Entertainment modes.

Firewall policy: Block most

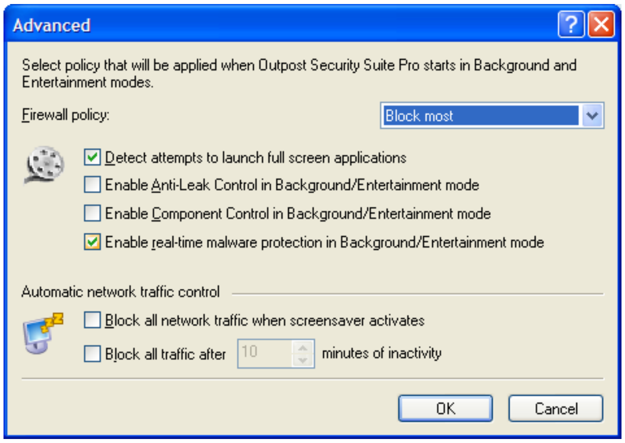
☑ Detect attempts to launch full screen applications
□ Enable Anti-Leak Control in Background/Entertainment mode
□ Enable Component Control in Background/Entertainment mode
☑ Enable real-time malware protection in Background/Entertainment mode

Automatic network traffic control

□ Block all network traffic when screensaver activates
□ Block all traffic after 10 minutes of inactivity

3.4 Inactivity Timers

Outpost Security Suite can act as a “screen saver” for your system’s network activity and block all network communications and traffic when the system is idle. This feature can help protect your system from unauthorized access when you’re not controlling it, or help prevent applications on your system from consuming network bandwidth when you’re not using your computer. To configure the inactivity timers, go to the **Tools** menu, click **Options** and click **Advanced** on the **Policy** tab.



Advanced

Select policy that will be applied when Outpost Security Suite Pro starts in Background and Entertainment modes.

Firewall policy: Block most

☑ Detect attempts to launch full screen applications
□ Enable Anti-Leak Control in Background/Entertainment mode
□ Enable Component Control in Background/Entertainment mode
☑ Enable real-time malware protection in Background/Entertainment mode

Automatic network traffic control

□ Block all network traffic when screensaver activates
□ Block all traffic after 10 minutes of inactivity

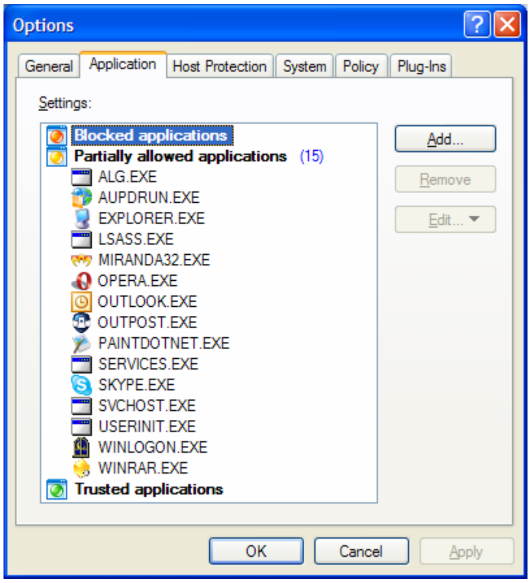
You can either choose to block all network traffic upon activation of your Windows screensaver, or you can specify the inactivity interval, after which network access is blocked.

3.5 Application Level Filtering

One of Outpost's most important features is application level filtering. This lets you decide which applications should have access and which should not.

The dialog window to control applications is accessed by right-clicking the system tray icon, selecting **Options** and then the **Application** tab.

This is the **Application** dialog window:



Settings:

- Blocked applications
- Partially allowed applications (15)
  - ALG.EXE
  - AUPDRUN.EXE
  - EXPLORER.EXE
  - LSASS.EXE
  - MIRANDA32.EXE
  - OPERA.EXE
  - OUTLOOK.EXE
  - OUTPOST.EXE
  - PAINTDOTNET.EXE
  - SERVICES.EXE
  - SKYPE.EXE
  - SVCHOST.EXE
  - USERINIT.EXE
  - WINLOGON.EXE
  - WINRAR.EXE
- Trusted applications

Outpost Security Suite divides all applications into three categories:

- **Blocked**—all activity of this group is blocked. We recommend that you add to this group all applications that do not need Internet access, such as text editors, calculators, etc.
- **Partially Allowed**—Outpost Security Suite allows access to the Internet for these applications based on the rules that were created by you manually or from presets. Only the specified application activity is allowed. We advise that you put most of your applications in this group.
- **Trusted**—all activity for these applications is allowed. It is not recommended that you include an application in this group unless you trust it absolutely.

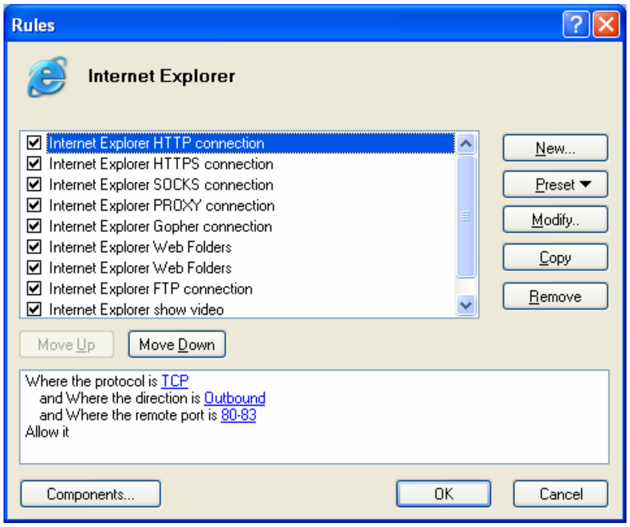
There is no need to add your applications to these groups manually. Rules Wizard automatically does this for you.

You can change an application's status between **Blocked, Partially allowed, and Trusted** at any time. Applications can simply be dragged and dropped from one category to another.

You can also directly add an application by dragging its icon from Windows Explorer or your desktop into the **Options** > **Application** dialog or by clicking on the **Add** button, then browsing to the location of the application's **.exe** file and clicking on the **Open** button. If the same application is already listed in another category, it will be deleted from that other category.

The **Edit** button lets you change any of the detailed settings for whatever application is highlighted.

Whenever an application is dragged to the **Partially allowed applications** category of the **Options' Application** tab, or is in any other way added to this category, the following dialog box with its list of rules is displayed:



Internet Explorer

☑ Internet Explorer HTTP connection
☑ Internet Explorer HTTPS connection
☑ Internet Explorer SOCKS connection
☑ Internet Explorer PROXY connection
☑ Internet Explorer Gopher connection
☑ Internet Explorer Web Folders
☑ Internet Explorer Web Folders
☑ Internet Explorer FTP connection
☑ Internet Explorer show video

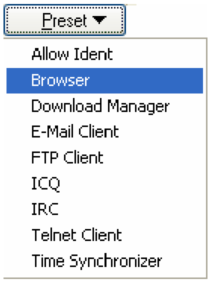
Where the protocol is TCP
and Where the direction is Outbound
and Where the remote port is 80-83
Allow it

Using this dialog, advanced users have full control of each of the different protocol settings by highlighting any one of these and pressing the **Modify** button. This is covered in detail in 5.4 Creating Rules for Applications.

A simpler approach is to use the **Preset** button to select the general type of application that best applies. The settings for these presets were designed by our engineers and are optimal for most purposes. Even advanced users are recommended to use these presets and then later tweak their settings as needed. In using the **Rules** dialog, an empty check box in the list of rules means that rule will not be applied.

Note: It is possible to create several different rules for the same application. Be aware that **Outpost Security Suite** uses the first instance of a rule that has criteria matching the application's activity and ignores all subsequent ones. The firewall rules are processed in the order in which they are listed. Once a rule is matched, searching of the rules list stops. Any other rules that match this type of communication are ignored, if they are further on the list than the first rule that matches. The buttons **Move Up** and **Move Down** are used to change the sequence of rules so you can determine which rule **Outpost** will use. If no rule is found, **Outpost Security Suite** displays the **Rules Wizard** dialog or simply blocks the connection, depending on whether you are running **Outpost** in **Rules Wizard** or **Block Most** mode.

Clicking the **Preset** button in the above dialog gives you choices that look like this:



The choices on the **Preset** list will very likely be added to as time goes on or otherwise modified. This will be included in any updates of the **Outpost Security Suite** software as was covered earlier. For advanced information about rule creation, see 5.4 Creating Rules for Applications.

3.6 Host Protection

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 (for example, 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 as harmful.

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

The current degree of protection is characterized by the local security level setting which represents the combination of specific Anti-Leak and Component Control settings providing this or that level of host security.

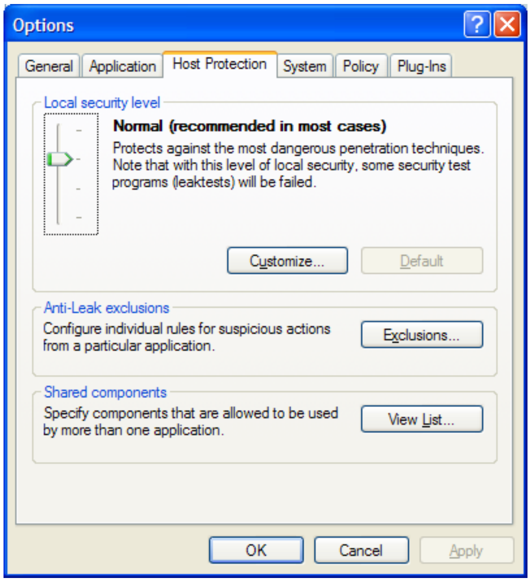
3.6.1 Setting Local Security Level

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

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

- **Advanced—**provides the best protection against all penetration techniques that are often used by malicious software to bypass firewall software. Having selected this level, you will get a lot of product prompts that require your response; therefore it is recommended for advanced users.

- **Normal—**ensures protection against the more dangerous techniques only and is recommended for most cases. However, if **Normal** security level is selected, some of the more exotic security test programs (leaktests) will be failed.
- **Low—**provides protection against the easiest penetration techniques only; the number of product prompts is minimal.
- **Disabled—**if you select this option, Host Protection is disabled completely.



Local security level

Normal (recommended in most cases)

Protects against the most dangerous penetration techniques. Note that with this level of local security, some security test programs (leaktests) will be failed.

Anti-Leak exclusions

Configure individual rules for suspicious actions from a particular application.

Shared components

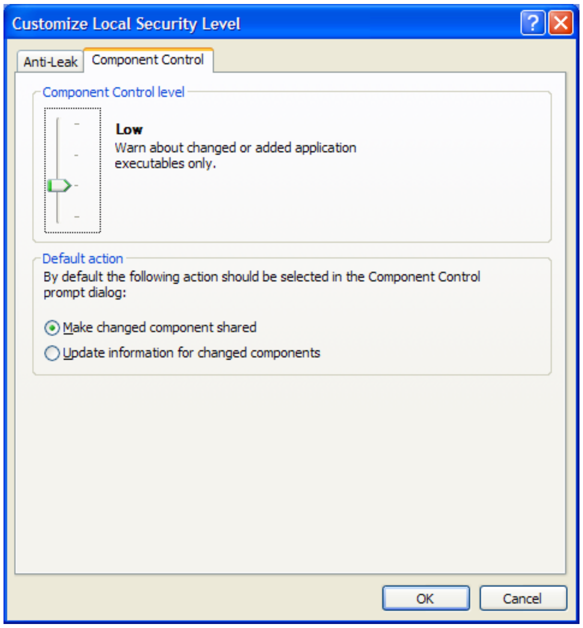
Specify components that are allowed to be used by more than one application.

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 and Component Control according to your specific requirements (see the corresponding sections below for details).

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

3.6.2 Component Control

Not only does **Outpost** monitor applications, but it also monitors the components of each application. So, when a module of an application has changed and the application is about to establish a connection, **Outpost Security Suite** will ask you whether it should be allowed. The purpose of this **Component Control** is to make sure components are not fake or malicious. Some Trojan horses can be inserted as modules of legitimate applications (for example, your browser is made up of many separate parts) and thus gain the privileges needed to go online. **Outpost Security Suite** allows you to set the desired Component Control level by selecting the **Host Protection** tab, click the **Customize** button under **Local security level** and select the **Component Control** tab:



Component Control level

Low
Warn about changed or added application executables only.

Default action

By default the following action should be selected in the Component Control prompt dialog:

● Make changed component shared

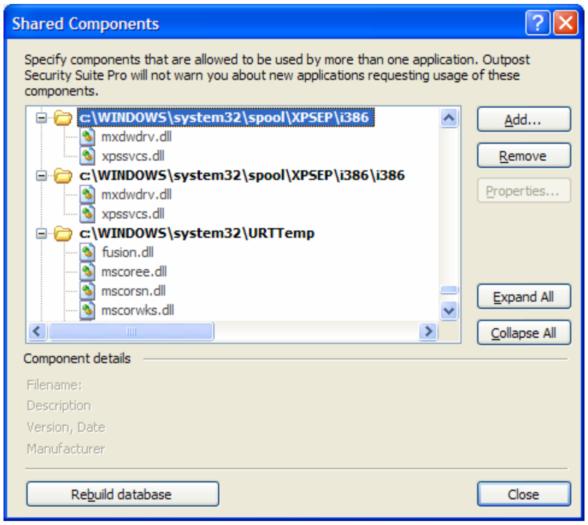
○ Update information for changed components

Select the desired component control level from the following options:

- **Maximum—Outpost Security Suite** will monitor all components that are being registered to be part of a legitimate application. **It is recommended that you use this option only when you suspect an unknown malware to exist in your system because this option may seriously impact on your system performance.**
- **Normal—Outpost Security Suite** will monitor all new components as they are being registered to be a part of an application yet are not located in the application folder. This option is suitable for most cases and provides a balance between security and performance.
- **Low**—the same as **Normal** but in this case Outpost Security Suite will not warn about every changed or added application component, but will warn only about executable files. It is recommended to use this option instead of completely disabling Component Control to keep the minimally necessary security level.
- **Disabled—**Turns **Component Control** off. This option is only recommended when you experience significantly reduced performance, crashes or other errors that lead to system instability. **Turning Component Control off severely reduces your system's security level.**

There are a number of components in each system that are always used by more than one application. Two examples are: Windows system libraries and common language runtime. Such components are typically trusted because it is known that they don't impose a threat; moreover, they are often used by many applications, and monitoring all these common components takes up a lot of system resources and reduces performance.

To optimize component control performance, **Outpost Security Suite** supports the **Shared Components** list to which you can add trusted components intended for use by more than one application. By default, all components located in the Windows installation folder and its subfolders are added to this list after you install **Outpost Security Suite**. Click **View list** to add or remove components.



Shared Components

Specify components that are allowed to be used by more than one application. Outpost Security Suite Pro will not warn you about new applications requesting usage of these components.

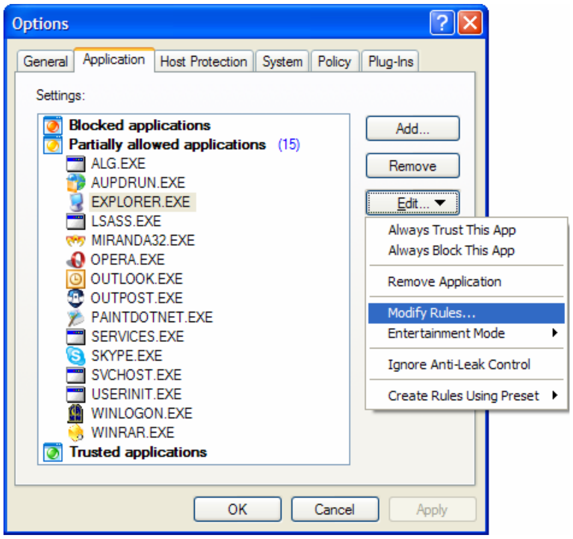
c:\WINDOWS\system32\spool\XPSEP\i386
mxdwdrv.dll
xpssvcs.dll
c:\WINDOWS\system32\spool\XPSEP\i386\i386
mxdwdrv.dll
xpssvcs.dll
c:\WINDOWS\system32\URTTemp
fusion.dll
mscoree.dll
mscorsn.dll
mscorwks.dll

Component details
Filename:
Description
Version, Date
Manufacturer

After you install a service pack, or other massive software update that affects a large number of common components, it is recommended that you **rebuild** the common components database so that **Outpost Security Suite** is aware of the changes made to your system configuration.

Note: After you click **Rebuild database**, all information about components that are manually added or modified will be lost.

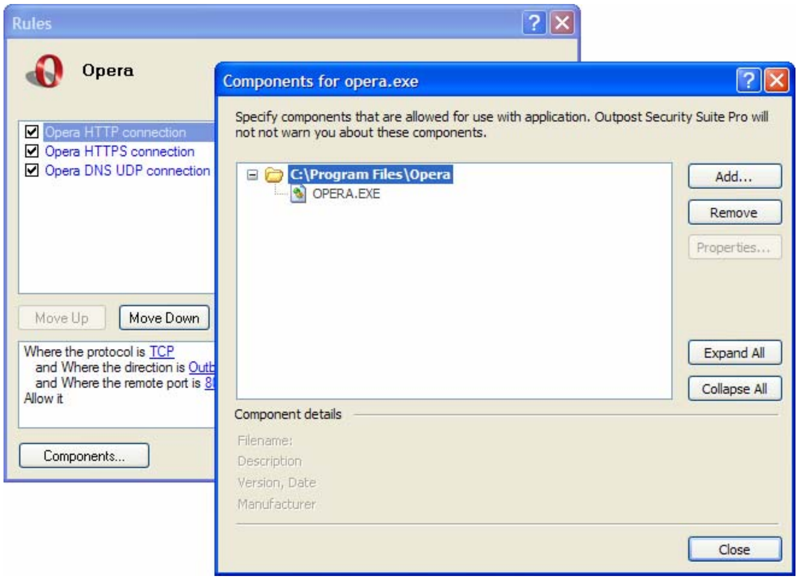
You can also view the components Outpost Security Suite monitors for each application by selecting the application from the list, selecting **Edit** > **Modify Rules** and clicking the **Components** button:



Options

Settings:

Blocked applications
Partially allowed applications (15)
ALG.EXE
AUPDRUN.EXE
EXPLORER.EXE
LSASS.EXE
MIRANDA32.EXE
OPERA.EXE
OUTLOOK.EXE
OUTPOST.EXE
PAINTDOTNET.EXE
SERVICES.EXE
SKYPE.EXE
SVCHOST.EXE
USERINIT.EXE
WINLOGON.EXE
WINRAR.EXE
Trusted applications



Specify components that are allowed for use with application. Outpost Security Suite Pro will not not warn you about these components.

- C:\Program Files\Opera
  - OPERA.EXE

Component details

Filename:
Description
Version, Date
Manufacturer

☑ Opera HTTP connection
☑ Opera HTTPS connection
☑ Opera DNS UDP connection

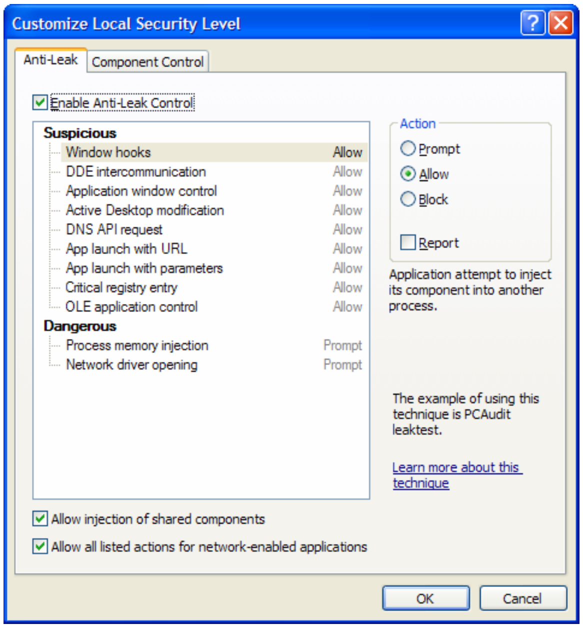
Where the protocol is TCP
and Where the direction is Outb
and Where the remote port is 8
Allow it

Tip: In a Rules Wizard prompt for the changed component, shared components are marked red and components of a specific application are marked green.

3.6.3 Anti-Leak Control

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

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



☑ Enable Anti-Leak Control

Suspicious	
Window hooks	Allow
DDE intercommunication	Allow
Application window control	Allow
Active Desktop modification	Allow
DNS API request	Allow
App launch with URL	Allow
App launch with parameters	Allow
Critical registry entry	Allow
OLE application control	Allow
Dangerous	
Process memory injection	Prompt
Network driver opening	Prompt

Action

○ Prompt
● Allow
○ Block

□ Report

Application attempt to inject its component into another process.

The example of using this technique is PCAudit leaktest.

Learn more about this technique

☑ Allow injection of shared components

☑ Allow all listed actions for network-enabled applications

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

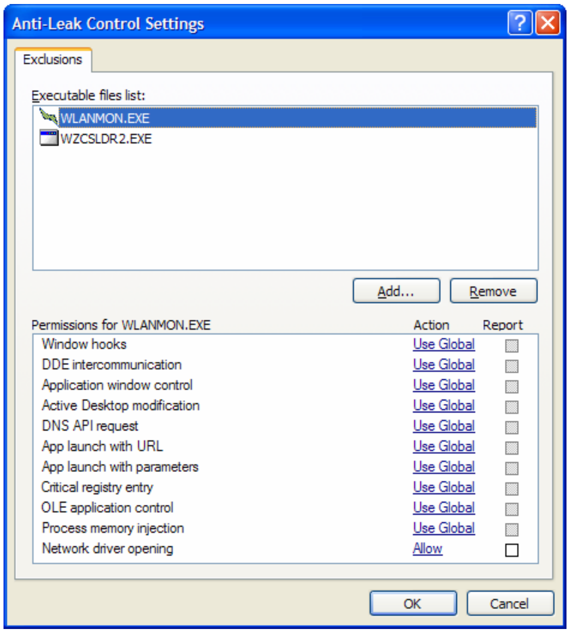
- **Prompt**. Outpost Security Suite will prompt you each time an application tries to perform the selected activity.
- **Allow**. The selected activity will always be allowed for all applications on your system.
- **Block**. The selected activity will always be blocked for all applications on your system.

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

Some applications use the technology of component injection (Windows hooks) for their common activity (Nvidia drivers, for example). If you use such applications and want to allow them to inject components from the shared components list into another process’s memory, select the **Allow injection of shared components** check box. This setting has a higher priority than the **Prompt/Block** settings for Windows hooks.

If you want to have full control over all system activity of applications installed on your computer, clear the **Allow all listed actions for network-enabled applications**, otherwise it has a higher priority than the **Prompt/Block** settings for all listed techniques.

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



Executable files list:

WLANMON.EXE
WZCSLDR2.EXE

Permissions for WLANMON.EXE	Action	Report
Window hooks	Use Global	□
DDE intercommunication	Use Global	□
Application window control	Use Global	□
Active Desktop modification	Use Global	□
DNS API request	Use Global	□
App launch with URL	Use Global	□
App launch with parameters	Use Global	□
Critical registry entry	Use Global	□
OLE application control	Use Global	□
Process memory injection	Use Global	□
Network driver opening	Allow	□

Click **OK** to save your settings.

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

Note: If you completely trust an application and want to allow it to perform all the listed actions, right-click the application in the list on the **Application** tab and select **Ignore Anti-Leak Control**. The application will be added to the Anti-Leak exclusions list with all actions set to **Allow**.

4 Plug-Ins

4.1 Introduction

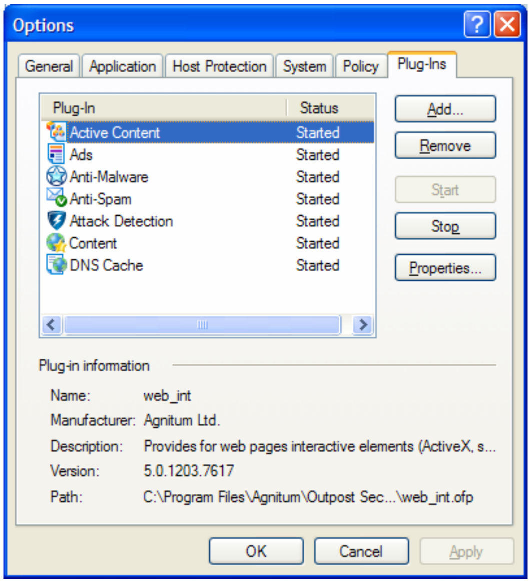
One of **Outpost Security Suite's** most useful and effective design strategies is the employment of plug-ins. These modules can be created by third-party developers and easily added to increase **Outpost Security Suite's** capabilities.

If you are interested in developing **Outpost Security Suite** plug-ins, please visit http://www.agnitum.com/products/outpost/developers.html for samples, tutorials and the developer's forum.

Please note that plug-ins are absolutely independent from each other and the main **Outpost Security Suite** module.

The dialog window to control these plug-ins is accessed from a right-click the system tray icon and selecting **Options** and then the **Plug-Ins** tab. You can also access this dialog from the main window using the menu **Options**, then selecting **Plug-Ins Setup**.

This is the **Plug-Ins** dialog window:



Plug-In	Status
Active Content	Started
Ads	Started
Anti-Malware	Started
Anti-Spam	Started
Attack Detection	Started
Content	Started
DNS Cache	Started

Plug-in information

Name: web_int
Manufacturer: Agnitum Ltd.
Description: Provides for web pages interactive elements (ActiveX, s...
Version: 5.0.1203.7617
Path: C:\Program Files\Agnitum\Outpost Sec...\web_int.ofp

The right-side buttons are:

- **Add—**used to add a new plug-in to **Outpost Security Suite** using Windows' file open dialog.
- **Remove—**used to delete a plug-in that is highlighted on the list.
- **Start—**starts a highlighted plug-in that is stopped.

- **Stop—**used to stop a highlighted plug-in from operating, but not to delete the plug-in from **Outpost Security Suite**.
- **Settings—**used to modify any of the settings for a highlighted plug-in. The types of settings vary with the different plug-ins.

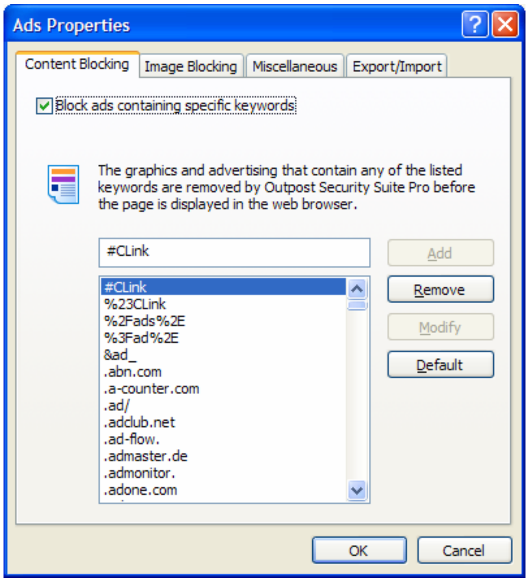
Note: Only those plug-ins having the status of “Started” can have their settings modified. The settings dialog for any started plug-in can also be accessed by clicking on that plug-in in the main window’s left panel and selecting **Properties** on the shortcut menu. The settings dialog for each started plug-in can also be accessed using the 🛠 ▾ button on the toolbar of **Outpost Security Suite’s** main window.

The **Plug-In information** section, in the lower half of the above dialog, shows the most important properties of a highlighted plug-in and where, on your system, the plug-in’s **.ofp** file is located.

4.2 Ad Blocking

More and more web sites are becoming filled with ads. With a fast connection these are generally not a problem but often it’s nice just to surf without the distraction of blinking, moving ads.

To change the settings of **Outpost Security Suite’s** ad blocking, right-click the system tray icon to get the shortcut menu, then select **Options** and go to the **Plug-Ins** tab. Click **Advertisement Blocking** to highlight it and then click the **Settings** button to get the following dialog:



☑ Block ads containing specific keywords

The graphics and advertising that contain any of the listed keywords are removed by Outpost Security Suite Pro before the page is displayed in the web browser.

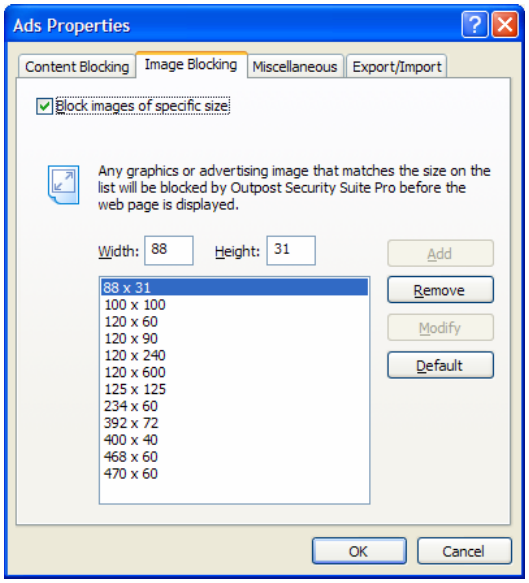
#CLink

#CLink
%23CLink
%2Fads%2E
%3Fad%2E
&ad_
.abn.com
.a-counter.com
.ad/
.adclub.net
.ad-flow.
.admaster.de
.admonitor.
.adone.com

Outpost Security Suite can block the display of banner ads from certain advertisers. As the picture shows, **Outpost Security Suite** comes with a large list of the most common words in Internet advertisement URLs located within the HTML tags “**<IMG SRC=**” and “**<A HREF=**”. To add another word to the list, simply start typing it in the text field above the list and click the **Add** button. **Outpost Security Suite** replaces any banners containing one of these words with the text: `[AD-IMG]`.

Be sure that **Block Ad content containing specific keywords** is selected. Click **Add** to add the new entry to the list or **Modify** to change it.

Outpost Security Suite can also block all banner ads having standard sizes. To do this, select the **Image Size** tab on the **Options** dialog. You will get the following display:



☑ Block images of specific size

Any graphics or advertising image that matches the size on the list will be blocked by Outpost Security Suite Pro before the web page is displayed.

Width: 88 Height: 31

88 x 31
100 x 100
120 x 60
120 x 90
120 x 240
120 x 600
125 x 125
234 x 60
392 x 72
400 x 40
468 x 60
470 x 60

Outpost Security Suite lets you block all specific sized graphic images that have a link. Be sure to select **Block images of specific size**.

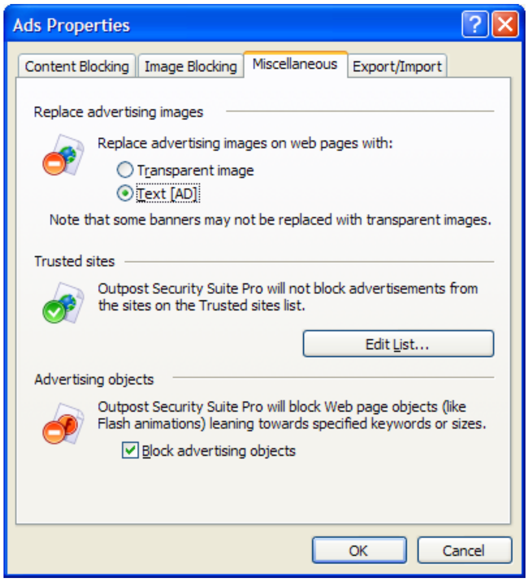
Immediately after installation, **Outpost Security Suite** is set to block all images with a link (images inside an <**a** tag) of 100 x 100, 125 X 125, 468 x 60, 470 x 60, 234 x 60, 120 x 80, and 88 x 31 pixels. By default **Outpost Security Suite** replaces the designated banners with the text **[AD]** in the web page.

To add to the list of image sizes to be blocked, type in the size of the image to be blocked and click the **Add** button.

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 addition, a few ads will not be blocked with these plug-in default settings.

To allow all graphics to be displayed on the screen, clear **Block images of specific size**.

Outpost Security Suite also allows you to specify whether to replace advertisements with text message **[AD]** or with **transparent images** of the same size as the ad and supports the **Trusted sites** list to which you can add Web sites with advertisements you do not want to be blocked. Click the **Miscellaneous** tab to alter these settings.



Replace advertising images

Replace advertising images on web pages with:

○ Transparent image

● Text [AD]

Note that some banners may not be replaced with transparent images.

Trusted sites

Outpost Security Suite Pro will not block advertisements from the sites on the Trusted sites list.

Advertising objects

Outpost Security Suite Pro will block Web page objects (like Flash animations) leaning towards specified keywords or sizes.

☑ Block advertising objects

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

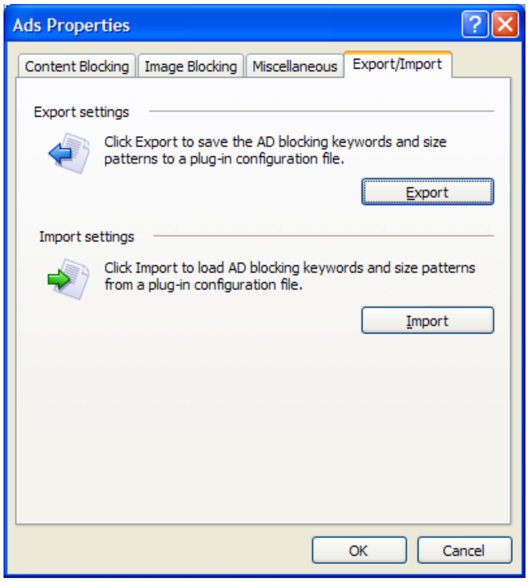
Modern Internet advertisements not only include graphic banners, they also use various ActiveX objects to display advertisements. The simplest example is Macromedia Flash movies, which are broadly used on web sites. Such advertisements consume a lot more system resources and network bandwidth than traditional banners and are not cut off by most standard banner removal software tools.

Outpost Security Suite can 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 filtering.

This way, **Outpost Security Suite** will block such objects either when it encounters an **<OBJECT>** tag—used to embed these objects into a web page—that contains any of the specified ad keywords, or when the size of the object display area matches one of the specified ad sizes.

All plug-in settings can be saved to a configuration file so you can reload them if you find that any modification proved unsatisfactory, or so you can easily transfer your settings to another computer.

To manage the plug-in configuration files, click the **Export/Import** tab in its properties dialog.



Click Export to save the AD blocking keywords and size patterns to a plug-in configuration file.

Click Import to load AD blocking keywords and size patterns from a plug-in configuration file.

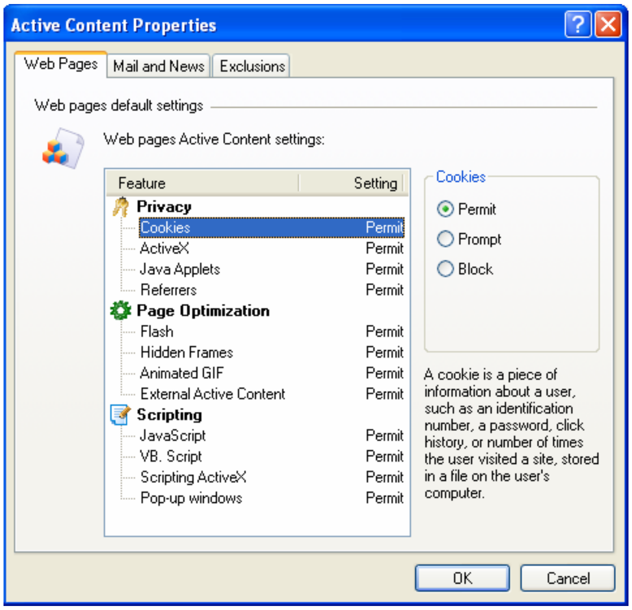
Click **Export** (to save) or **Import** (to load) and then specify the configuration file name.

4.3 Active Content Blocking

The **Active Content Filtering** plug-in controls the operation of the following active elements:

- ActiveX
- Java applets
- Programs based on Java Script and VBScript
- Cookies
- Pop up windows
- Referrers
- Hidden frames
- Flash animations
- Animated GIF images
- Scripting ActiveX elements
- Page navigation scripts

This plug-in lets you independently allow or block any of these elements that might be contained in the web pages you are browsing.



Web pages default settings

Web pages Active Content settings:

Feature	Setting
Privacy	
Cookies	Permit
ActiveX	Permit
Java Applets	Permit
Referrers	Permit
Page Optimization	
Flash	Permit
Hidden Frames	Permit
Animated GIF	Permit
External Active Content	Permit
Scripting	
JavaScript	Permit
VB. Script	Permit
Scripting ActiveX	Permit
Pop-up windows	Permit

Cookies

● Permit
○ Prompt
○ Block

A cookie is a piece of information about a user, such as an identification number, a password, click history, or number of times the user visited a site, stored in a file on the user's computer.

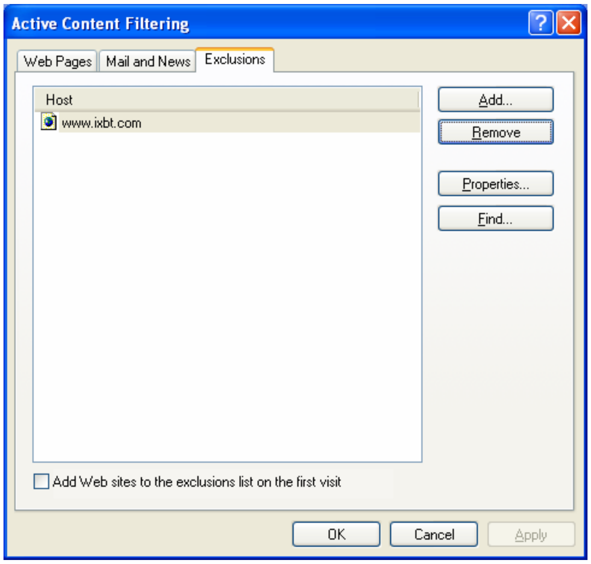
Interactive elements treatment can be independently configured for e-mail, news and web pages. Click either **Mai1 and News** or **Web Pages** tab and select the element type to block. The right part of the window will show you the element description and the setting for each selection.

The following settings are available:

- **Block—**blocks the element’s action.
- **Prompt—**asks you each time this element attempts to activate.
- **Permit—**allows the element to function.

Note: The use of all active elements is enabled for all web pages by default.

To configure individual settings for specific web sites, select the **Exclusions** tab:



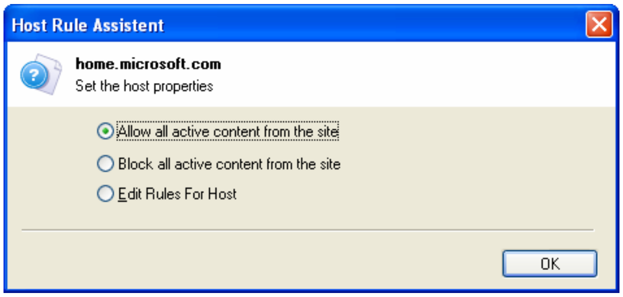
Host
www.ixbt.com

□ Add Web sites to the exclusions list on the first visit

Click **Add** and type the site address (that has active content settings) that you want to personalize and click **OK**.

The site that you just added is immediately given all the default active content settings. Click **Properties** to change specific settings that will apply to this site only.

Note: If you want to be able to individually configure each of the sites you visit, select the **Add web sites to the exclusions list on the first visit** to have **Outpost Security Suite** display the Host Rules Assistant window each time a web page is first visited:

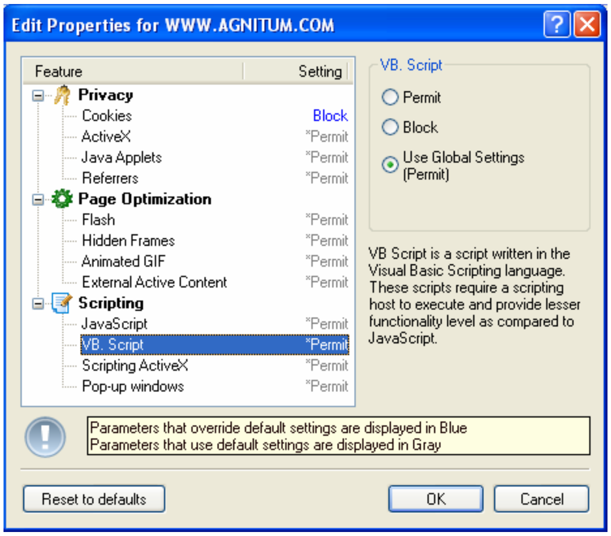


Host Rule Assistent

home.microsoft.com
Set the host properties

● Allow all active content from the site
○ Block all active content from the site
○ Edit Rules For Host

Whether you select to **Allow** or **Block all active content from the site** the site will be simply added to the exclusions list. Select **Edit host settings** to display the **Edit Properties** dialog (see below) in which you can customize the specific site's active content treatment settings.



Edit Properties for WWW.AGNITUM.COM

Feature	Setting
Privacy	
Cookies	Block
ActiveX	*Permit
Java Applets	*Permit
Referrers	*Permit
Page Optimization	
Flash	*Permit
Hidden Frames	*Permit
Animated GIF	*Permit
External Active Content	*Permit
Scripting	
JavaScript	*Permit
VB. Script	*Permit
Scripting ActiveX	*Permit
Pop-up windows	*Permit

VB. Script

○ Permit
○ Block
● Use Global Settings (Permit)

VB Script is a script written in the Visual Basic Scripting language. These scripts require a scripting host to execute and provide lesser functionality level as compared to JavaScript.

Parameters that override default settings are displayed in Blue
Parameters that use default settings are displayed in Gray

The site can inherit the settings from the global policy or you can assign each an individual value.

Note: Settings that inherit default values are displayed in gray; settings that are assigned unique values are displayed in blue.

Tip: This dialog can also be invoked by selecting a site on the **Exclusions** tab and clicking the **Properties** button.

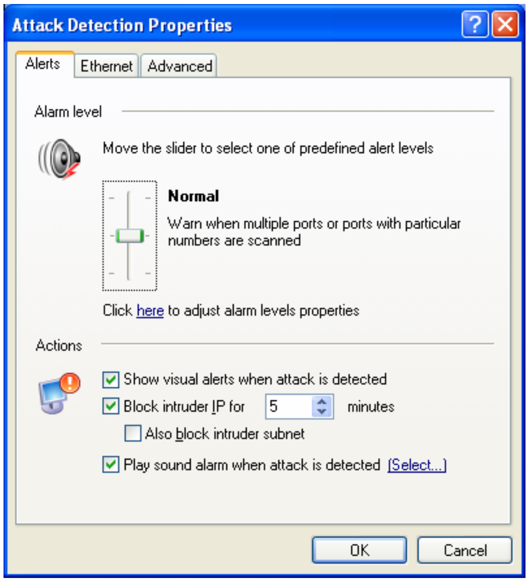
Some sites require that all or several of its active content elements be active for their pages to display or function correctly. If you make the settings for all sites very restrictive, you can experience the following problems: images not being displayed, a web page not showing at all, a web page displayed incorrectly or some useful services contained in applets not working. If this happens with only a few sites, just change this plug-in's settings for those sites by adding them to the exclusions list as described above; otherwise you may need to loosen the default active content treatment policy.

4.4 Attack Detection

This plug-in informs you of a possible attack on your computer from the Internet or the network your computer is connected to. It recommends the steps to be taken as well, in order to prevent damage to your computer.

The **Attack Detection** plug-in lets you specify the conditions in which a warning is to be displayed. It also has response settings that will be used if a specified security level is exceeded.

Below is the plug-in's **Options** dialog window:



Alarm level

Move the slider to select one of predefined alert levels

Normal

Warn when multiple ports or ports with particular numbers are scanned

Click here to adjust alarm levels properties

Actions

☑ Show visual alerts when attack is detected

☑ Block intruder IP for 5 minutes

□ Also block intruder subnet

☑ Play sound alarm when attack is detected [Select...]

In the section named **Alarm level**, you move the slider up or down for a higher or lower alert level:

- **High**—an **"Attack Detection"** alert is displayed even if a single scanning of your port is detected.
- **Normal**—an **"Attack Detection"** alert is displayed if several ports are scanned or if a specific port is scanned that **Outpost Security Suite** recognizes as one that is commonly used in attacks.
- **Low**—an **"Attack Detection"** alert warning is displayed if a multiple attack is definitely detected.

You can adjust suspicious packets threshold for each of the levels by clicking the appropriate link. This will bring you the dialog window where you can specify the exact number of suspicious packets that are considered as an attack.

Specify the steps **Outpost Security Suite** is to follow if an attack on your computer is detected:

- **Show visual alerts when attack is detected—**if selected, **Outpost Security Suite** will display alert message every time an attack is detected.
- **Play sound alarm when attack is detected—**if selected, **Outpost Security Suite** will play the specified audio file every time an attack is detected.
- **Block intruder IP for—**if selected, blocks all network exchanges from the computer attacking yours for the number of minutes you set (60 minutes by default).
    - **Also block intruder subnet—**if selected, blocks all network exchanges from the entire subnet to which the intruder belongs.

Ethernet Attacks

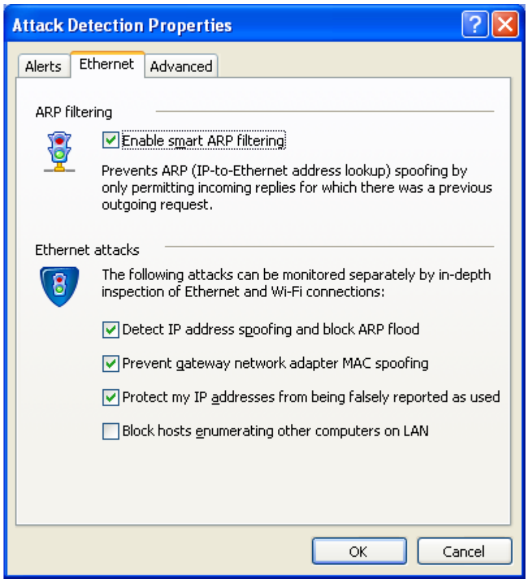
When data is sent from one computer to another over a local network, the sending machine broadcasts an ARP (IP-to-Ethernet address lookup) request to determine the MAC address based on the IP address of the target machine and waits for it to send back its MAC address. During the time between the packet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

Attack Detection plug-in also detects and averts particular Ethernet attacks such as IP spoofing, ARP scanning, ARP flood and others by inspecting Ethernet and Wi-Fi connections thus protecting your system from invasions on a local network. To specify the Ethernet attacks prevention settings, select the Ethernet tab in the plug-in properties window. The following options are available:

- **Enable smart ARP filtering**. Prevents ARP spoofing - where a node starts sending a huge number of ARP replies with varying MAC addresses in a short time span, trying to overload the network equipment as it tries to determine which MAC address actually belongs to the node. If enabled, Outpost Security Suite only permits incoming replies from other hosts for which there was a previous outgoing request. Only the first ARP reply is accepted for each request. Smart ARP filtering also protects from ARP cache poisoning, which occurs when someone succeeds in intercepting Ethernet traffic using fake ARP replies in an effort to change the address of a network card to one that an attacker can monitor. Additionally, it prevents ARP floods - where a huge number of bogus ARP replies are sent to the target machine freezing a system.
- **Detect IP address spoofing and block IP flood**. Detects when an attacker falsifies or forges his IP address and blocks abnormal volumes of traffic which may otherwise overload a computer. This option cannot stop the network from being flooded but can protect the PC from overload.
- **Prevent gateway network adapter MAC spoofing**. Detects any attempt by an attacker to associate a gateway network adapter IP address with their own MAC address to allow them to intercept packets. Hackers can substitute legitimate MAC

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

- **Protect my IP addresses from being false reported as used**. Detects cases where two or more hosts share the same IP address. This can be due to an attacker attempting to gain access to network traffic or block a computer from accessing the network, but could also happen legitimately where an ISP uses multiple servers for load-sharing. If enabled, Outpost Security Suite blocks ARP replies that have the same IP (but different MAC's) and thus protects computer from the IP address duplication consequences.
- **Block hosts enumerating other computers on LAN**. Limits the number of ARP requests enumerating IP addresses from one MAC address during a specified time interval which can imply network scanning. Some massively propagating viruses use mass host enumeration to hop from one computer to another, infecting them as they go. This technique is also used by scanners and vulnerability analyzers.



ARP filtering

☑ Enable smart ARP filtering

Prevents ARP (IP-to-Ethernet address lookup) spoofing by only permitting incoming replies for which there was a previous outgoing request.

Ethernet attacks

The following attacks can be monitored separately by in-depth inspection of Ethernet and Wi-Fi connections:

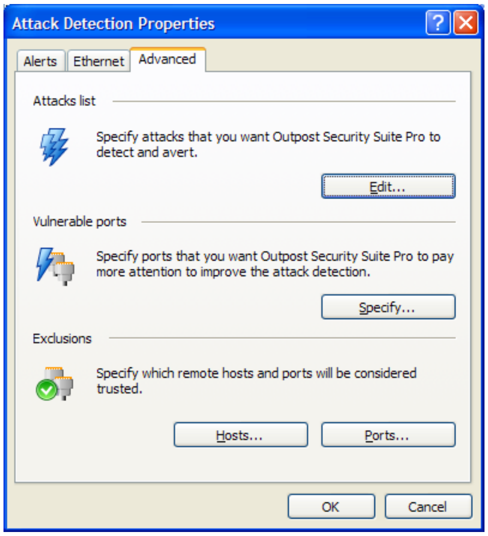
☑ Detect IP address spoofing and block ARP flood

☑ Prevent gateway network adapter MAC spoofing

☑ Protect my IP addresses from being falsely reported as used

☐ Block hosts enumerating other computers on LAN

You can also select attacks that Outpost Security Suite is to detect and avert. By default Outpost Security Suite handles more than fifteen types of attacks and exploits, but you can choose to not detect certain attack types in order to eliminate frequent false positive alert messages that may be appearing if a service in your network, for example, acts like an attack source.



Attacks list

Specify attacks that you want Outpost Security Suite Pro to detect and avert.

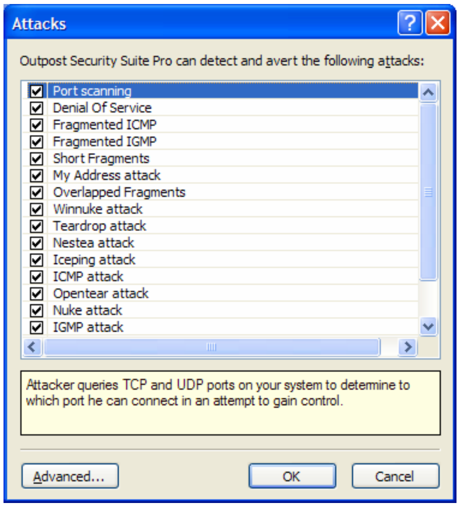
Vulnerable ports

Specify ports that you want Outpost Security Suite Pro to pay more attention to improve the attack detection.

Exclusions

Specify which remote hosts and ports will be considered trusted.

Click the **Advanced** tab of the plug-in settings dialog and then click **Edit list** to display the **Attacks** dialog box.

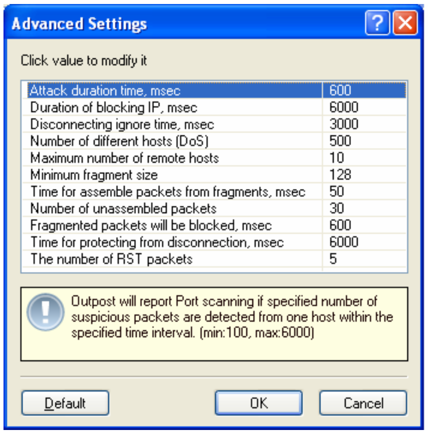


Outpost Security Suite Pro can detect and avert the following attacks:

- ☑ Port scanning
- ☑ Denial Of Service
- ☑ Fragmented ICMP
- ☑ Fragmented IGMP
- ☑ Short Fragments
- ☑ My Address attack
- ☑ Overlapped Fragments
- ☑ Winnuke attack
- ☑ Teardrop attack
- ☑ Nestea attack
- ☑ Iceping attack
- ☑ ICMP attack
- ☑ Opentear attack
- ☑ Nuke attack
- ☑ IGMP attack

Attacker queries TCP and UDP ports on your system to determine to which port he can connect in an attempt to gain control.

Here you can select the attacks you want **Outpost Security Suite** to detect and avert. Note that the **Advanced** button displays a dialog that lets you change the settings that apply to **all attacks in the list**.



Click value to modify it

Attack duration time, msec	600
Duration of blocking IP, msec	6000
Disconnecting ignore time, msec	3000
Number of different hosts (DoS)	500
Maximum number of remote hosts	10
Minimum fragment size	128
Time for assemble packets from fragments, msec	50
Number of unassembled packets	30
Fragmented packets will be blocked, msec	600
Time for protecting from disconnection, msec	6000
The number of RST packets	5

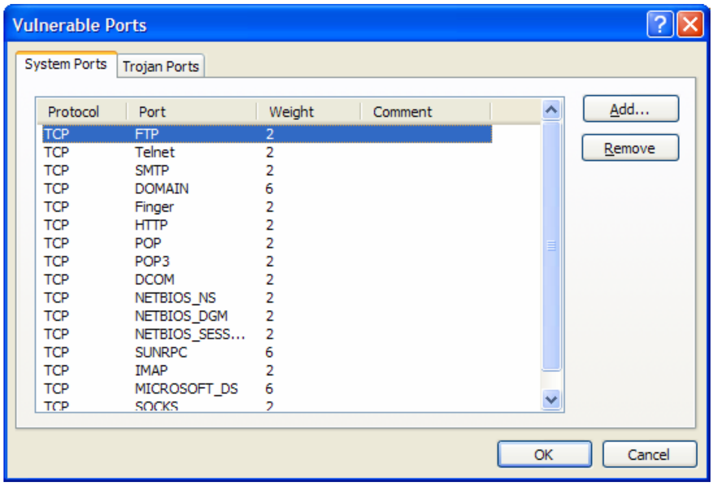
Outpost will report Port scanning if specified number of suspicious packets are detected from one host within the specified time interval. (min:100, max:6000)

To change the setting value, highlight the setting in the list and click its value in the right column.

Note: Alter these settings with care since an improper attack detection configuration can lead to significant problems with your system network connectivity.

From a security point of view TCP and UDP ports in your system are divided into several groups according to the probability of an attacker using the port to break in. Attempt to access ports assigned to vulnerable services like DCOM or RPC with a higher probability is an inidication that you are being probed then access to a regular port.

However, you may have custom services assigned to custom ports that are also tempting for an attacker. **Outpost Security Suite** lets you create a list of such ports to which it will pay more attention while monitoring network traffic. To manage the list of vulnerable ports, click the **Advanced** tab in the plug-in settings dialog and then in **Vulnerable ports** click **Specify**.



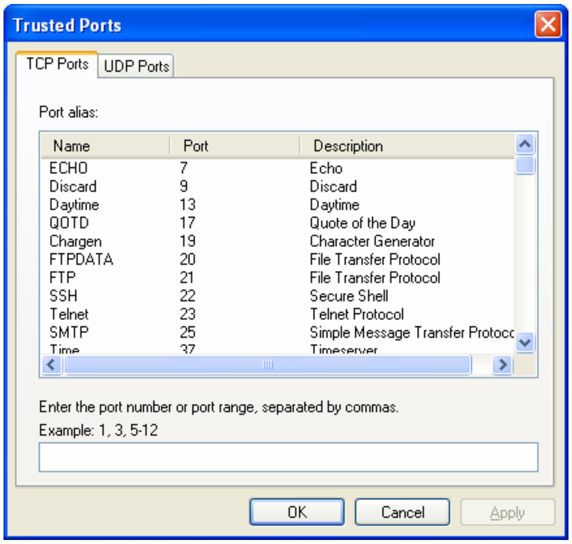
Protocol	Port	Weight	Comment
TCP	FTP	2	
TCP	Telnet	2	
TCP	SMTP	2	
TCP	DOMAIN	6	
TCP	Finger	2	
TCP	HTTP	2	
TCP	POP	2	
TCP	POP3	2	
TCP	DCOM	2	
TCP	NETBIOS_NS	2	
TCP	NETBIOS_DGM	2	
TCP	NETBIOS_SESS...	2	
TCP	SUNRPC	6	
TCP	IMAP	2	
TCP	MICROSOFT_DS	6	
TCP	SOCKS	2	

Vulnerable ports are divided in two groups: System and Trojan. System ports list contains ports that are used by vulnerable system services; Trojan ports list contains ports that are exploited by well known Trojan horses. Click the tab according to the list you want to change.

Click **Add** and specify the **Protocol**, **Port number** and **Weight**. Weight is a decimal value that indicates port importance. A greater number indicates a more vulnerable port. You may also add comments to describe the port's purpose or anything you wish to note.

There can be computers on your network that you are absolutely sure are not a source of danger for your system, as well as ports on your system you are sure cannot serve as an intruder's backdoor. In other words, you consider that monitoring these hosts and/or ports is fruitless and wish to conserve your system's resources and increase its performance by not monitoring them.

The **Outpost Security Suite Attack Detection** plug-in features exclusion lists to which you can add hosts and ports you don't want to have monitored. To manage these lists, click **Hosts** or **Ports** under **Exclusions** in the **Advanced** tab of the plug-in settings dialog.



Port alias:

Name	Port	Description
ECHO	7	Echo
Discard	9	Discard
Daytime	13	Daytime
QOTD	17	Quote of the Day
Chargen	19	Character Generator
FTPDATA	20	File Transfer Protocol
FTP	21	File Transfer Protocol
SSH	22	Secure Shell
Telnet	23	Telnet Protocol
SMTP	25	Simple Message Transfer Protocc
Time	37	Timeserver

Enter the port number or port range, separated by commas.
Example: 1, 3, 5-12

4.5 DNS Cache

The Internet works by assigning a series of numbers to each computer connected to it. This is called the computer's IP address. An example of an IP address is: 64.176.127.178. You can simply type in this series of numbers into your browser's location field (near the top of your browser's window) and press your keyboard's Enter key and your browser will go to that computer's web pages.

Although these numerical IP addresses are easy for a computer to use, they are difficult for us humans to remember. So an address system was invented that uses words or letters called the DNS (Domain Name System). A DNS name is what you are probably more familiar with than IP numbers. An example of a DNS name is: www.agnitum.com.

DNS names are much easier for us to remember, but our browsers still need to use the IP address to find and transfer files on the Internet. Therefore, there are databases throughout the Internet that keep track of what IP address goes with what DNS name. To find the IP address that corresponds to a DNS name, sometimes your browser has to consult several different databases located at different places on the Internet and this often takes time.

To speed things up, **Outpost Security Suite**vides a personalized look-up table of DNS addresses on your own computer. This is called a domain name cache and you can customize it however you like.

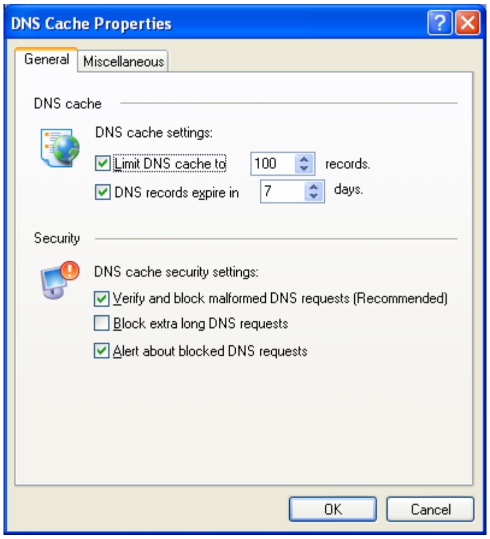
Outpost Security Suite maintains the DNS cache automatically within your specifications to include those addresses that are most recently used by you. The amount of time that a DNS address is saved in the DNS cache depends on the time you specify as one of the settings for this plug-in. It also depends on how many DNS names you want **Outpost Security Suite** to keep track of. Only the most recently used names are kept up to the maximum number of entries you specify.

Make sure the **Enable DNS caching** is selected on the plug-in's shortcut menu for Outpost Security Suite to provide this speed up.

To modify the settings of the **DNS Cache** plug-in, select **Properties** on the same menu.

You can limit the DNS database to a specific number of entries and have them be automatically deleted if they are not used within a certain number of days. To not limit the database to only those entries that are used within a certain number of days, clear the **DNS records expire** check box.

To enhance your system security, **DNS Cache** plug-in blocks invalid or malformed DNS requests that might cause system crash or serve as an exploit of a DNS backdoor. Select **Verify and block malformed DNS requests** option to have **DNS Cache** plug-in block these requests so that an attacker or a malicious program would not have chance to exploit DNS flaws in your system. Also, you can set to block extra long DNS requests, which can be an attempt to send out your private data as the domain name of a forth or higher level. To do that, select the **Block extra long DNS requests** check box. Additionally, you may want to receive pop-up alerts about such requests, if you want to stay informed about DNS attacks against your system. To receive alerts, select the **Alert about blocked DNS requests** check box.



DNS cache

DNS cache settings:

☑ Limit DNS cache to 100 records.

☑ DNS records expire in 7 days.

Security

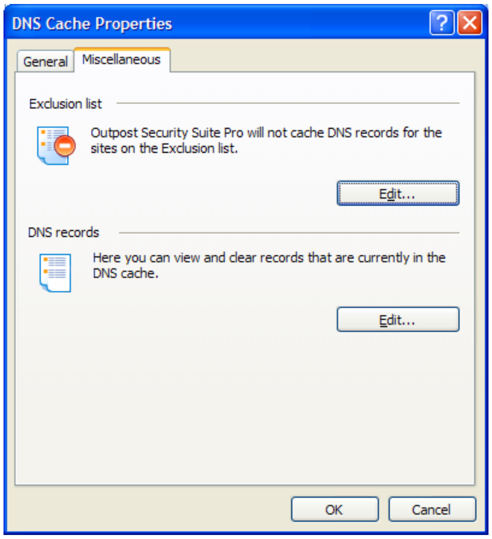
DNS cache security settings:

☑ Verify and block malformed DNS requests (Recommended)

□ Block extra long DNS requests

☑ Alert about blocked DNS requests

The list of already cached site names and their IP addresses can be managed in the DNS records dialog that you can invoke by selecting the **Miscellaneous** tab and clicking **Edit list** under **DNS records**:



Exclusion list

Outpost Security Suite Pro will not cache DNS records for the sites on the Exclusion list.

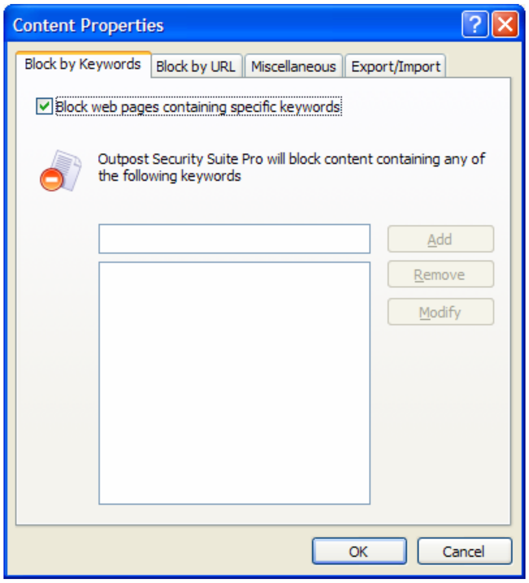
DNS records

Here you can view and clear records that are currently in the DNS cache.

DNS Cache also provides you an **Exclusion list** to which you can add site names that you don't want to be cached. This list is especially useful when you frequently access sites that have IP addresses that change often or you experience other problems when accessing specific sites from your computer. To manage the list, click the **Edit list** button under **Exclusion list**.

4.6 Content Filtering

Using the **Content** plug-in, you can block the display of particular web sites or pages containing objectionable material. To do this, select **Properties** on the plug-in's shortcut menu:

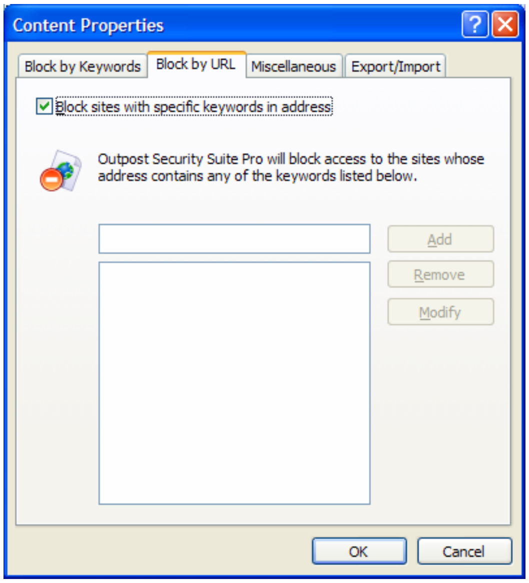


☑ Block web pages containing specific keywords

Outpost Security Suite Pro will block content containing any of the following keywords

Select **Block content containing specific keywords,** as shown in the picture above, then start typing into the text field (above the large listing area) each word you want Outpost to look for to block web pages containing those words. As soon as you start typing, the **Add** button is activated. Click the **Add** button for each word or phrase you want to add to the list. Any web page containing any of the words on this list will not be displayed.

To list particular web sites you do not want displayed on your computer, select the **Block by URL** tab:

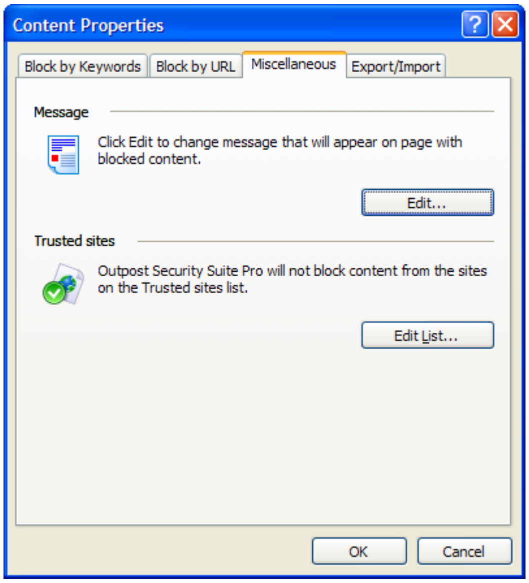


☑ Block sites with specific keywords in address

Outpost Security Suite Pro will block access to the sites whose address contains any of the keywords listed below.

Select **Block sites with specific keywords in address** as shown in the picture. Type in the URL or the part of the URL of the site you do not want displayed on your computer. As soon as you start typing, the **Add** button is activated. Click the **Add** button after you finish typing in the URL of each site to be blocked. Then click the **OK** button to have **Outpost Security Suite** save the list.

To change the message that will appear instead of any pages with objectionable materials click **Miscellaneous**, then click the **Edit** button:



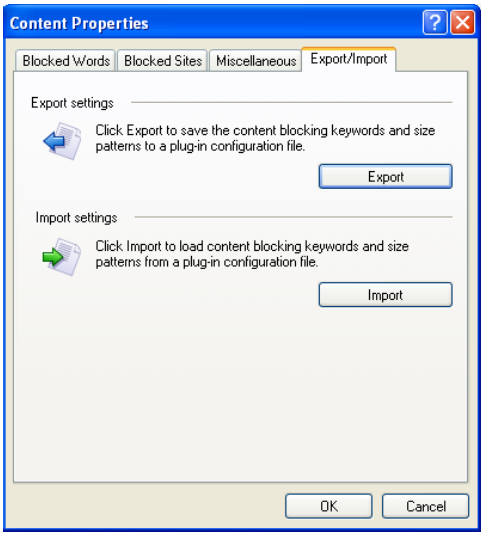
Click Edit to change message that will appear on page with blocked content.

Outpost Security Suite Pro will not block content from the sites on the Trusted sites list.

Outpost Security Suite also supports the **Trusted sites** list to which you can add web sites which content you do not want to be blocked.

All plug-in settings can easily be saved to a configuration file so that you will further be able to load your settings back if you alter them in an inappropriate way, or transfer these settings to another computer.

To manage the plug-in configuration files, click **Export/Import** tab from its **Options** dialog.



Export settings

Click Export to save the content blocking keywords and size patterns to a plug-in configuration file.

Click Import to load content blocking keywords and size patterns from a plug-in configuration file.

Click **Export** or **Import** according to the action you need to take and then specify the configuration file name.

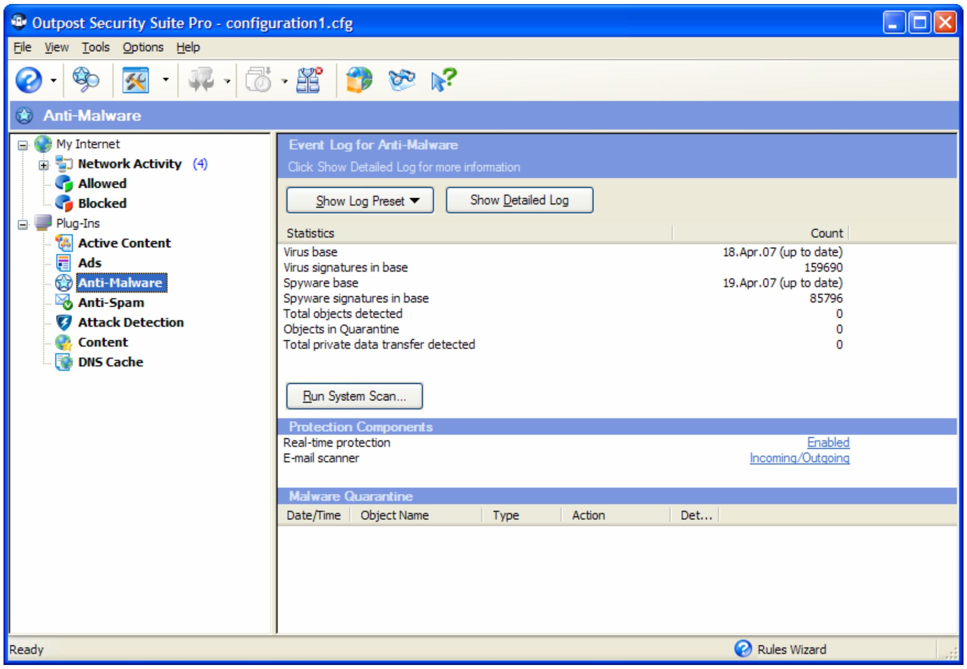
4.7 Anti-Malware

Malware is a growing problem that has affected many personal computer users. In increasing frequency users are confronted (unknowingly generally) by malicious programs that infect their systems, collect information about their web surfing stats, their computers' installed applications and other private data that is sent to third persons afterwards, spyware that tracks their actions without their consent. Malware can change e-mail texts, modify files on your hard disk, display annoying ads, 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.

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.

4.7.1 Performing System Scan

If you did not perform the system scan during Outpost Security Suite installation, it is recommended to run full scan just after 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.



Event Log for Anti-Malware

Click Show Detailed Log for more information

Statistics	Count
Virus base	18.Apr.07 (up to date)
Virus signatures in base	159690
Spyware base	19.Apr.07 (up to date)
Spyware signatures in base	85796
Total objects detected	0
Objects in Quarantine	0
Total private data transfer detected	0

Protection Components

Real-time protection	Enabled
E-mail scanner	Incoming/Outgoing

Malware Quarantine

Date/Time	Object Name	Type	Action	Det...

The wizard will help you specify the scanning settings and guide you through the whole process of the system scan.

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

Quick system scan. This option allows performing a fast scan of your system, checking the weakest points. Recommended for every day usage. The following items will be scanned during this check:

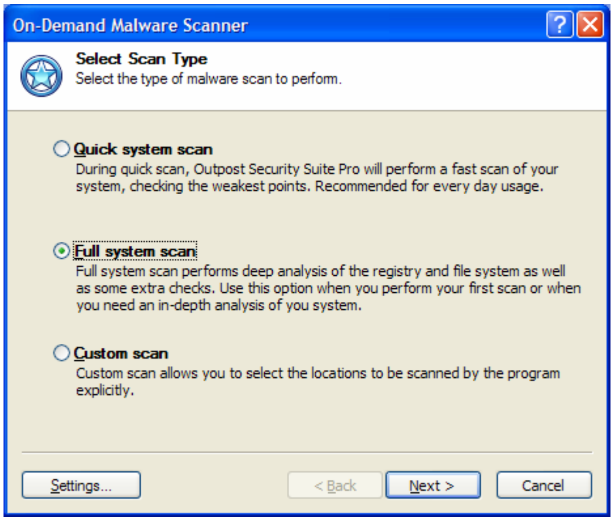
- Processes in memory
- Vulnerable registry keys
- Vulnerable files and folders (such as system %systemroot% folder, root %systemdrive% folder and Program Files)

Full system scan. Full system scan performs deep analysis of the registry and file system as well as some extra checks. The following will be performed during this check:

- Processes in memory check
- Full registry scan
- Full files and folders scan on non-removable disks (with explicitly specified drive letters; mounted disks are considered as folders)
- Cookies scan
- Startup entries scan

This check should be performed once you're scanning your system for the first time. The operation can take considerable time.

Custom scan. This option allows you to select the locations to be scanned by the program explicitly. You can select among the options stated above, and additionally, granularly select what to scan on your file system.



Select Scan Type
Select the type of malware scan to perform.

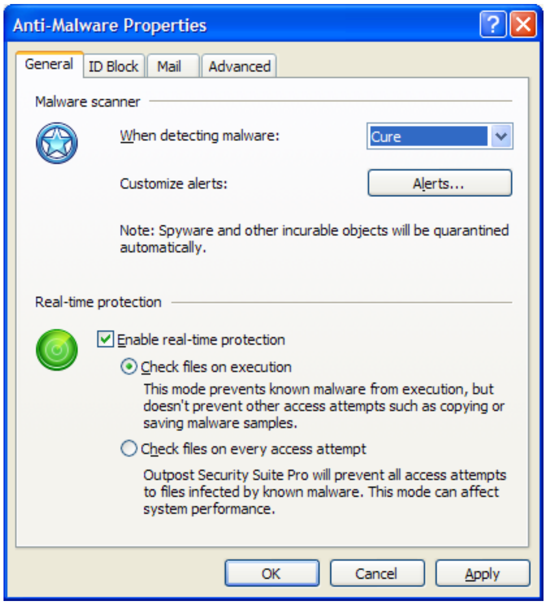
○ Quick system scan
During quick scan, Outpost Security Suite Pro will perform a fast scan of your system, checking the weakest points. Recommended for every day usage.

● Full system scan
Full system scan performs deep analysis of the registry and file system as well as some extra checks. Use this option when you perform your first scan or when you need an in-depth analysis of you system.

○ Custom scan
Custom scan allows you to select the locations to be scanned by the program explicitly.

The scanner will treat the detected objects according to the settings specified in the plug-in properties. To change the current settings, click the **Settings** button in the left lower corner of the wizard window. The plug-in properties window will be displayed allowing you to configure scanner behavior—specify an action to perform over the found malware, scanning exclusions, etc. The following actions can be performed on detecting a suspicious program:

- **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.
- **Cure**. On detecting a suspicious program, Outpost Security Suite Pro will try to cure the corresponding object. In case it is not possible to cure the object, it will be automatically quarantined.
- **Quarantine**. Outpost Security Suite Pro will place the detected malware in the quarantine.



Malware scanner

When detecting malware: Cure

Customize alerts:

Note: Spyware and other incurable objects will be quarantined automatically.

Real-time protection

☑ Enable real-time protection

● Check files on execution

This mode prevents known malware from execution, but doesn't prevent other access attempts such as copying or saving malware samples.

○ Check files on every access attempt

Outpost Security Suite Pro will prevent all access attempts to files infected by known malware. This mode can affect system performance.

For **Cure** and **Quarantine** actions, you can set the visual alerts to be displayed and sound alerts to be played on detecting the malware by clicking the **Alerts** button and selecting the corresponding check boxes. Outpost Security Suite Pro will display visual alert and play the specified sound file each time the malware is detected and cured/quarantined. This allows to get to know which programs you run and sites you visit pose you under the risk.

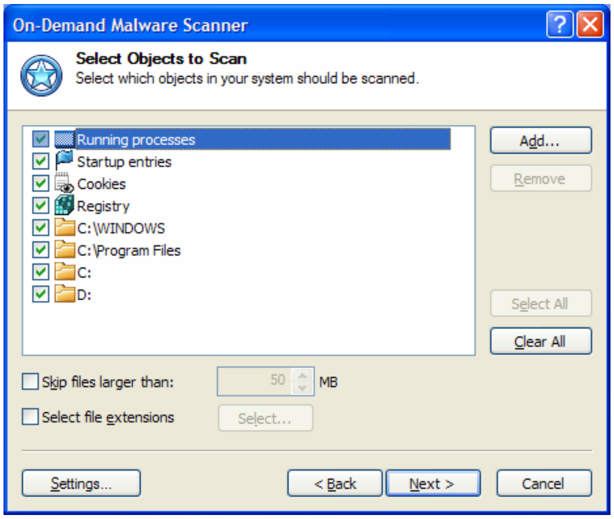
Tip: To improve scan performance, you can set Outpost Security Suite Pro to create scan status cache files in each scanned folder by selecting the **Enable SmartScan technology** check box on the **Advanced** tab of the plug-in properties. Note, that the cache files are invisible and therefore may cause false positives from anti-rootkit tools. To clear the cache, click **Clear Cache** button.

Note: Spyware objects are always considered incurable and automatically quarantined.

The specified action does not affect critical objects and cookies. If some critical object or cookie is detected during scanning, no action will be undertaken and the **Specify Actions for Detected Objects** step will be displayed after the scan is finished as if the **List All** action is selected.

Irrespective of the specified action, all the malware activity is blocked immediately after it is detected.

Select the scan type and click **Next**. If the **Custom scan** is selected, the **Select Objects to Scan** step appears allowing you to explicitly select the objects to be scanned.



On-Demand Malware Scanner

Select Objects to Scan

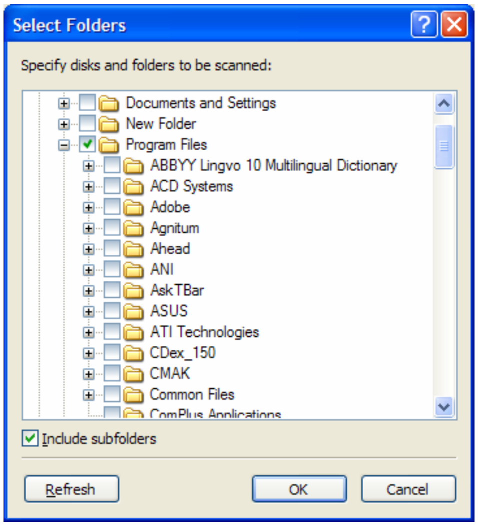
Select which objects in your system should be scanned.

- ☑ Running processes
- ☑ Startup entries
- ☑ Cookies
- ☑ Registry
- ☑ C:\WINDOWS
- ☑ C:\Program Files
- ☑ C:
- ☑ D:

□ Skip files larger than: 50 MB

□ Select file extensions

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**.



Select Folders

Specify disks and folders to be scanned:

- □ Documents and Settings
- □ New Folder
- ☑ Program Files
  - □ ABBYY Lingvo 10 Multilingual Dictionary
  - □ ACD Systems
  - □ Adobe
  - □ Agnitum
  - □ Ahead
  - □ ANI
  - □ AskTBar
  - □ ASUS
  - □ ATI Technologies
  - □ CDex_150
  - □ CMAK
  - □ Common Files
  - □ ComPlus Applications

☑ Include subfolders

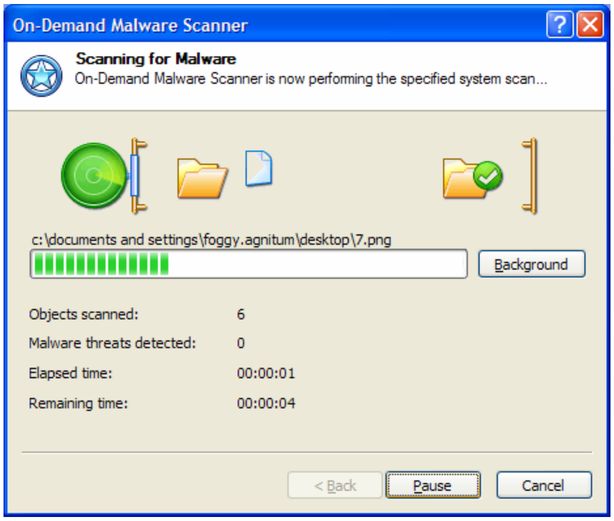
If you do not want to scan files of specific size, select the **Skip files larger than** check box and specify desirable file size. You can also constrain the scan to the specified types of files only by selecting the **Select file extensions** check box. To edit the list of file extensions to process, click the **Extensions** button. The most common types of files that could 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.

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.

The scanning process can run in background mode. If you want to work with Outpost Security Suite Pro while the scan is underway, click the **Background** button and the wizard will be minimized to the progress bar on the Information Panel. To see the full window again, click **Show Wizard**.

To abort a scan and see its results at any time, click **Cancel**.



On-Demand Malware Scanner

Scanning for Malware

On-Demand Malware Scanner is now performing the specified system scan...

c:\documents and settings\foggy.agnitum\desktop\7.png

Objects scanned: 6

Malware threats detected: 0

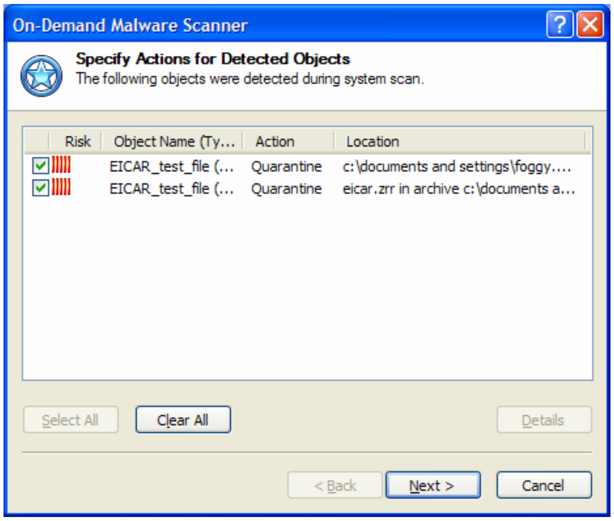
Elapsed time: 00:00:01

Remaining time: 00:00:04

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.



On-Demand Malware Scanner

Specify Actions for Detected Objects

The following objects were detected during system scan.

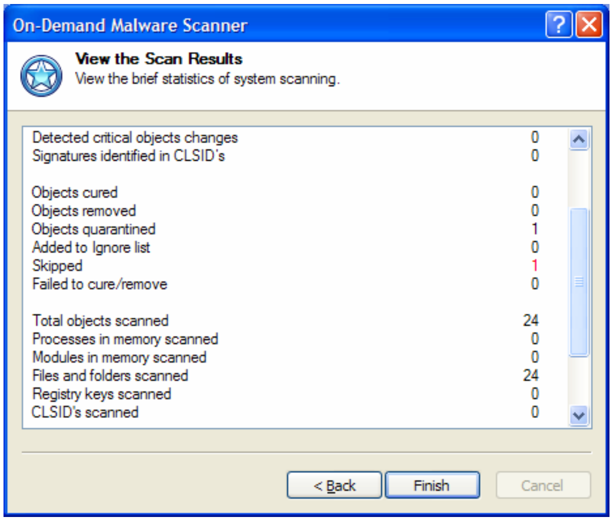
	Risk	Object Name (Ty...	Action	Location
☑	▮▮▮▮▮	EICAR_test_file (...	Quarantine	c:\documents and settings\foggy....
☑	▮▮▮▮▮	EICAR_test_file (...	Quarantine	eicar.zrr in archive c:\documents a...

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.

Tip: In the case you know about some of the found programs that they are not a sort of malware but a legitimate software and do not want Outpost Security Suite Pro to treat them as spyware or viruses (for example, you want to see ads displayed by some adware program), you can add such programs to exclusions. Outpost Security Suite Pro will ignore the programs on the list displaying no alerts on detecting their activity. Also these programs will not be displayed in the list of detected spyware. To add a program to exclusions, right-click its name and select **Add to Exclusions**. You can later remove program from the exclusions list using the Edit button on the **Advanced** tab of plug-in properties.

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.



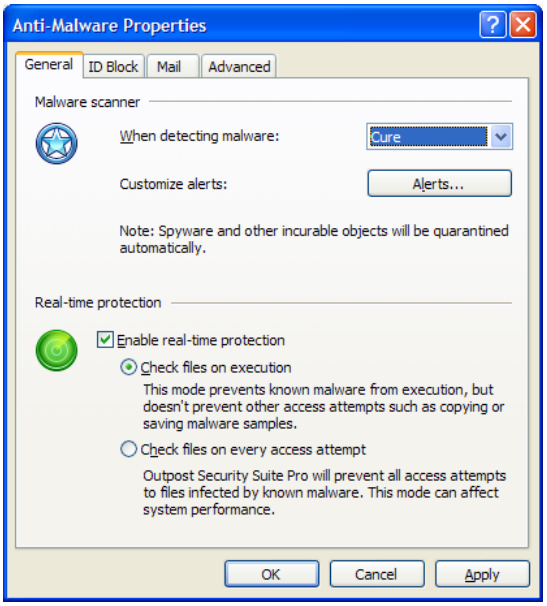
View the Scan Results
View the brief statistics of system scanning.

Detected critical objects changes	0
Signatures identified in CLSID's	0
Objects cured	0
Objects removed	0
Objects quarantined	1
Added to Ignore list	0
Skipped	1
Failed to cure/remove	0
Total objects scanned	24
Processes in memory scanned	0
Modules in memory scanned	0
Files and folders scanned	24
Registry keys scanned	0
CLSID's scanned	0

4.7.2 Real-Time Protection

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.


Anti-Malware Properties

General | ID Block | Mail | Advanced

Malware scanner

When detecting malware: Cure

Customize alerts: Alerts...

Note: Spyware and other incurable objects will be quarantined automatically.

Real-time protection

☑ Enable real-time protection

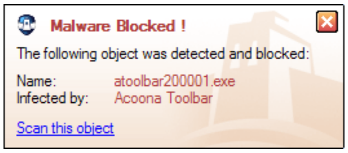
● Check files on execution

This mode prevents known malware from execution, but doesn't prevent other access attempts such as copying or saving malware samples.

○ Check files on every access attempt

Outpost Security Suite Pro will prevent all access attempts to files infected by known malware. This mode can affect system performance.

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

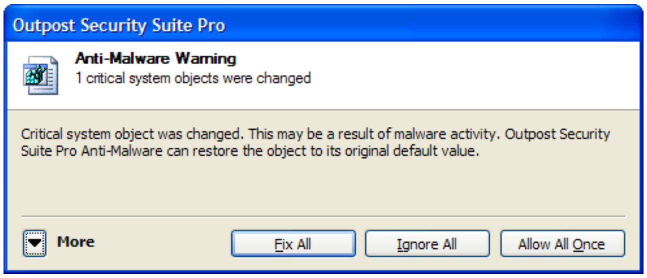

Malware Blocked !

The following object was detected and blocked:

Name: atoolbar200001.exe
Infected by: Acoona Toolbar

Scan this object

On detecting a critical system object change, Outpost Security Suite Pro the prompt dialog box will be displayed to the user asking him for an action to perform.


Outpost Security Suite Pro

Anti-Malware Warning
1 critical system objects were changed

Critical system object was changed. This may be a result of malware activity. Outpost Security Suite Pro Anti-Malware can restore the object to its original default value.

The following actions are available in the prompt:

- **Fix All**. Reverts the detected changes to critical system objects and quarantines the changed entries so you could restore them in case the changes are legitimate.

- **Ignore All**. If you consider the detected changes as legitimate and do not want Outpost Security Suite Pro to treat them as spyware-driven (for example, you are installing some software which registers its components in the system), you can set Outpost Security Suite Pro to stop controlling these critical objects by clicking **Ignore All**. Outpost Security Suite Pro will not monitor the changes of these objects anymore and will display no alerts on detecting their change. You can later set them back to be monitored by clicking the **Objects** button on the **Advanced** tab of plug-in properties and selecting the corresponding check boxes.
- **Allow Once**. Allows the detected change once. The next time the same change will be detected, the same prompt window will be displayed.

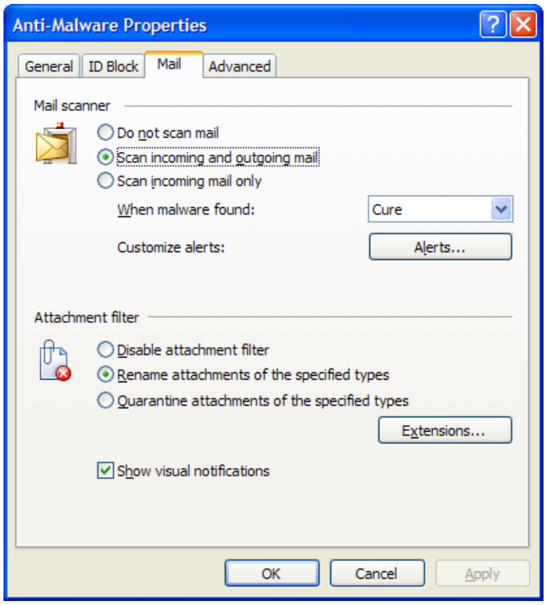
If you want, you can view the list of detected changes and perform the actions selectively by clicking the **More** button, highlighting the object in the list and clicking the action link by its side.

4.7.3 Scanning Mail Attachments

One of the simplest ways for worms, Trojans, and other malware to get to 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 launch the file attached to a received e-mail and the worm or virus starts performing its malicious actions resulting in system infection and malfunction.

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

To configure mail scanner, right-click the Anti-Malware plug-in in the left panel of the product main window and select **Properties**. On the **Mail** tab, select **Scan incoming and outgoing mail** or **Scan incoming mail only** according to your needs. Also specify the action to perform over malware detected in your e-mail by selecting **Cure** or **Quarantine** in the **When malware found** list.



Anti-Malware Properties

General | ID Block | Mail | Advanced

Mail scanner

○ Do not scan mail
● Scan incoming and outgoing mail
○ Scan incoming mail only

When malware found: Cure

Customize alerts: Alerts...

Attachment filter

○ Disable attachment filter
● Rename attachments of the specified types
○ Quarantine attachments of the specified types

Extensions...

☑ Show visual notifications

OK Cancel Apply

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

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

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

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

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 it and put in Outpost Security Suite Pro quarantine.

To edit the list of file extensions to process, click the **Extensions** button. The most common types of files that could 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 be notified about filter actions, select the **Show visual notifications** check box.

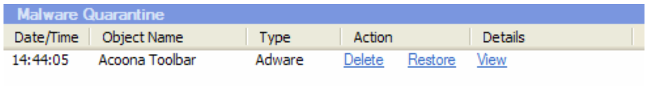
If you do not want the filter to rename or quarantine any attachments, select the **Disable attachment filter** option button.

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

4.7.4 Malware Quarantine

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

To have Outpost Security Suite Pro put all detected during system scan items into quarantine, open the plug-in properties, **General** tab and select **Quarantine** in the **When detecting malware** list. When this action is selected, you can see quarantined objects in the **Malware Quarantine** in the main Outpost Security Suite Pro window. Every malware program and object is represented in the quarantine list only once despite the number of separate signatures detected. For each object quarantined the date and time, as well as location and type are displayed.



Malware Quarantine

Date/Time	Object Name	Type	Action			Details
14:44:05	Acoona Toolbar	Adware	Delete	Restore	View	

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

For files infected by 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 allows to view the file contents without damaging the system.

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

To view the details for the quarantined object, click **View**. In the displayed window the object description and detailed information about locations of all related objects is shown.

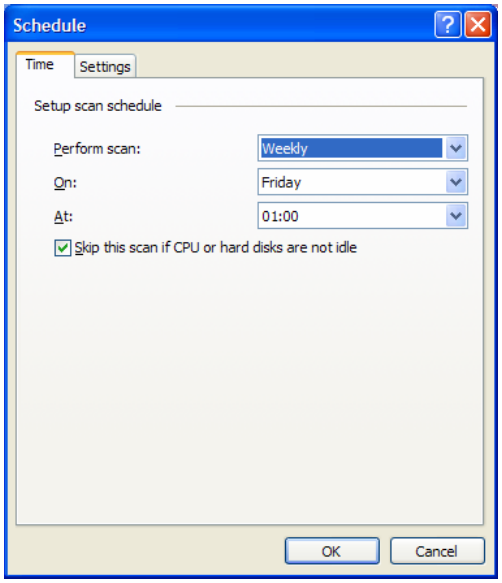
Note: There are some spyware programs that cannot be placed into quarantine.

4.7.5 Scheduling System Scan

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

To set a scheduled scan, right-click Anti-Malware plug-in, select **Properties**, select the **Advanced** tab, and click **Schedule**.

On the **Time** tab, you can specify a scan schedule. To setup the frequency of malware scans, use the **Perform scan** list. If you select **Weekly** scanning, you can also specify a day and the exact time when Outpost Security Suite Pro will scan the system; within daily scanning you can specify the time of the day to perform scanning. Select **Never** to disable scheduled scans.



Setup scan schedule

Perform scan: Weekly

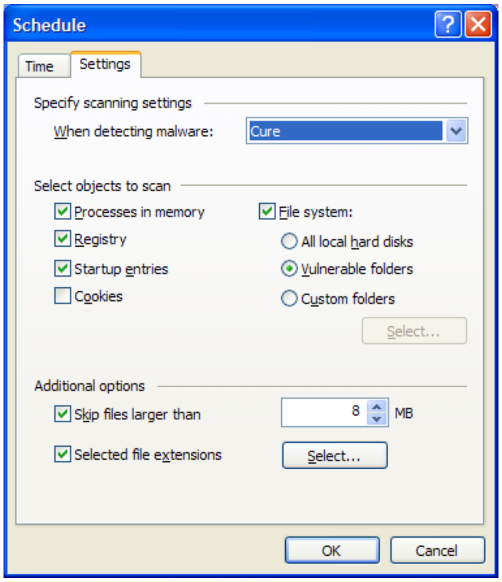
On: Friday

At: 01:00

☑ Skip this scan if CPU or hard disks are not idle

If you do not want the system scan to start when the computer performs some critical activity, select the **Skip this scan if CPU or hard disks are not idle** check box.

On the **Settings** tab, you can specify the scan settings: the action to perform when malware is detected, locations to scan in, etc. The settings are pretty much the same as you can specify in On-Demand Malware Scanner. See this section for details.



Specify scanning settings

When detecting malware: Cure

Select objects to scan

☑ Processes in memory

☑ Registry

☑ Startup entries

☐ Cookies

☑ File system:

○ All local hard disks

● Vulnerable folders

○ Custom folders

Additional options

☑ Skip files larger than 8 MB

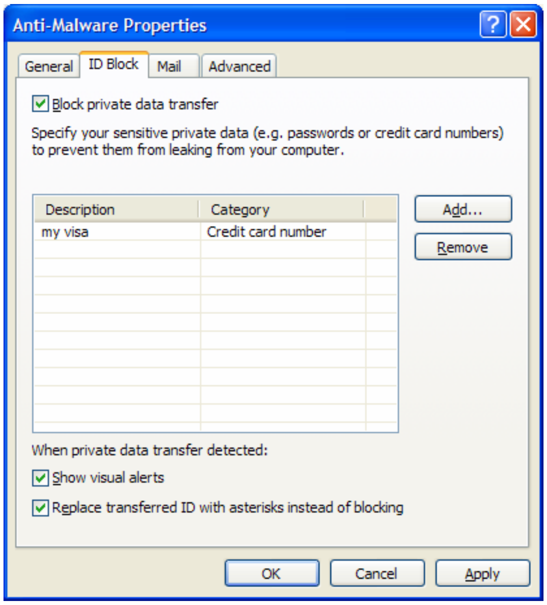
☑ Selected file extensions

Click **OK** after making your selections to save settings. Outpost Security Suite Pro will launch system scan according to the specified schedule.

4.7.6 ID Block

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

To protect your private data, select the **ID Block** tab of the plug-in properties window, and select the Block private data transfer check box. Click **Add** and under **Data to protect** enter any combination of symbols, letters or digits you do not want to leak from your computer. Specify the description to identify the string later and the category it regards to. After clicking **OK** and applying changes, that string will be blocked from any outgoing communication.



☑ Block private data transfer

Specify your sensitive private data (e.g. passwords or credit card numbers) to prevent them from leaking from your computer.

Description	Category
my visa	Credit card number

When private data transfer detected:

☑ Show visual alerts

☑ Replace transferred ID with asterisks instead of blocking

You can set to display alerts each time an attempt to transfer one of the specified strings to the network is performed by selecting the **Show visual alert** check box. If you select the **Replace transferred ID with asterisks instead of blocking** check box, any requester will receive only the "*" symbols which replace the original entry.

4.8 Anti-Spam

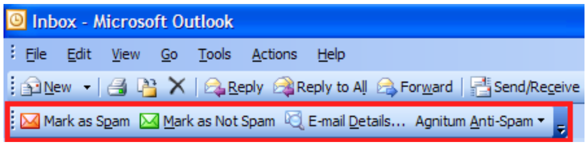
Without a doubt, every Internet user who actively uses e-mail in his everyday activities in the last several years has encountered the problem of unsolicited mass e-mail distribution, known as spam. Especially if they gave their e-mail address to public distribution lists or bulletin boards. The amount 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.

4.8.1 Training Anti-Spam

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.

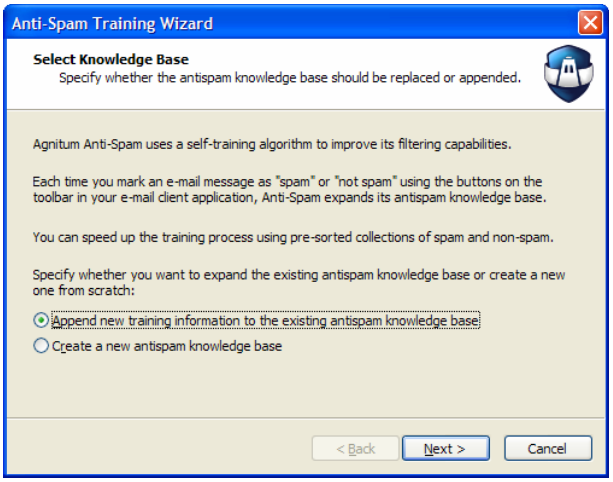
Manual training is based on your use of the **Mark as Spam** and **Mark as Not Spam** buttons on the Anti-Spam toolbar in your mail client. When you receive unsolicited e-mail, don't just delete it; mark it as spam by clicking on the **Mark as Spam** button. Anti-Spam processes the e-mail and learns 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.



Select Knowledge Base

Specify whether the antispam knowledge base should be replaced or appended.

Agnitum Anti-Spam uses a self-training algorithm to improve its filtering capabilities.

Each time you mark an e-mail message as "spam" or "not spam" using the buttons on the toolbar in your e-mail client application, Anti-Spam expands its antispam knowledge base.

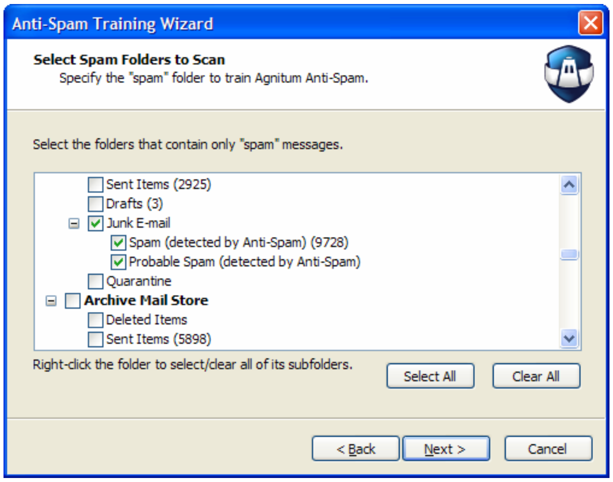
You can speed up the training process using pre-sorted collections of spam and non-spam.

Specify whether you want to expand the existing antispam knowledge base or create a new one from scratch:

● Append new training information to the existing antispam knowledge base

○ Create a new antispam knowledge base

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.



Anti-Spam Training Wizard

Select Spam Folders to Scan

Specify the "spam" folder to train Agnitum Anti-Spam.

Select the folders that contain only "spam" messages.

- ☐ Sent Items (2925)
- ☐ Drafts (3)
- ⊟ ☑ Junk E-mail
  - ☑ Spam (detected by Anti-Spam) (9728)
  - ☑ Probable Spam (detected by Anti-Spam)
- ☐ Quarantine
- ⊟ ☐ **Archive Mail Store**
  - ☐ Deleted Items
  - ☐ Sent Items (5898)

Right-click the folder to select/clear all of its subfolders.

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

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

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

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

Tip: If you consider all messages that are sent off from your computer as legitimate (a reasonable assumption), you can use these to train Anti-Spam. To set the filter to mark all outgoing messages as "not spam", select the **Train Anti-Spam on my outgoing e-mail also** check box on the **General** tab of Anti-Spam settings.

4.8.2 How Does the Bayesian Filtering Work?

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

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

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

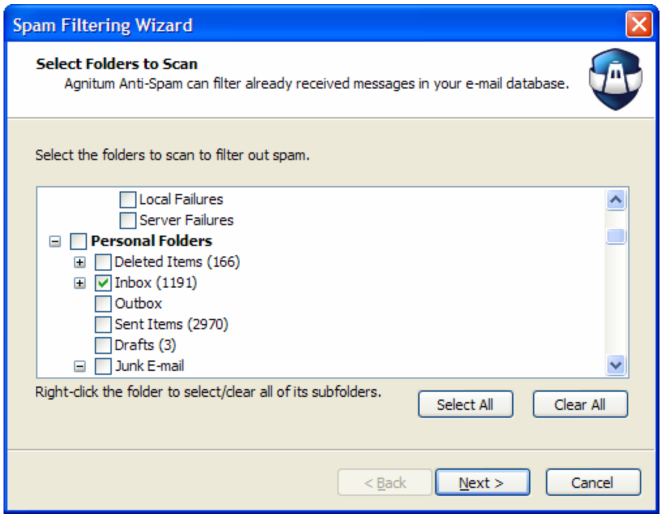
The probability that a message is spam (an overall message rank) is computed using the rankings of all the non-neutral words in the message (words with weight) based on Bayes' theorem and is a number in the range of 0 to 100. Zero means definitely not spam and 100 means definitely spam. If the message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

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

4.8.3 Scanning Mail Folders

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

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



Spam Filtering Wizard

Select Folders to Scan

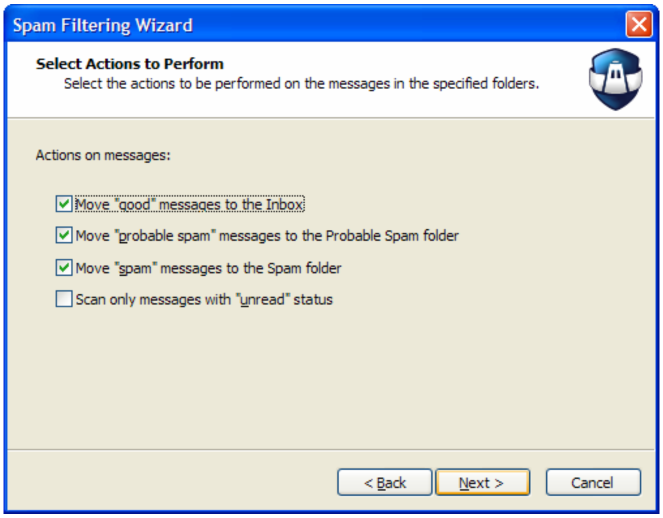
Agnitum Anti-Spam can filter already received messages in your e-mail database.

Select the folders to scan to filter out spam.

- □ Local Failures
- □ Server Failures
- □ **Personal Folders**
  - □ Deleted Items (166)
  - ☑ Inbox (1191)
  - □ Outbox
  - □ Sent Items (2970)
  - □ Drafts (3)
  - □ Junk E-mail

Right-click the folder to select/clear all of its subfolders.

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



Spam Filtering Wizard

Select Actions to Perform

Select the actions to be performed on the messages in the specified folders.

Actions on messages:

☑ Move "good" messages to the Inbox

☑ Move "probable spam" messages to the Probable Spam folder

☑ Move "spam" messages to the Spam folder

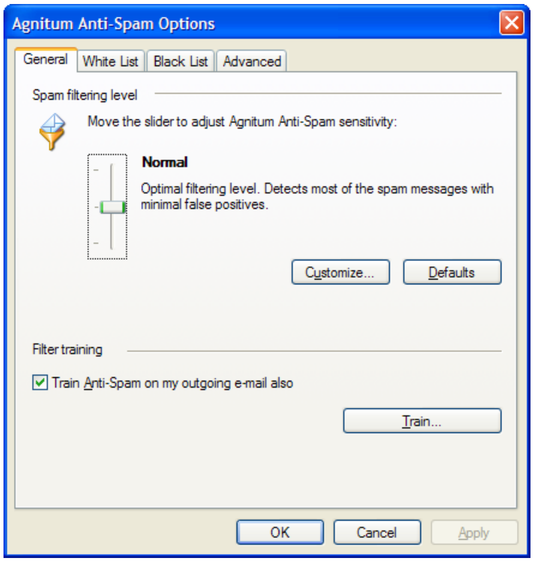
□ Scan only messages with "unread" status

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

4.8.4 Setting the Filtering Level

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

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


Agnitum Anti-Spam Options

Spam filtering level

Move the slider to adjust Agnitum Anti-Spam sensitivity:

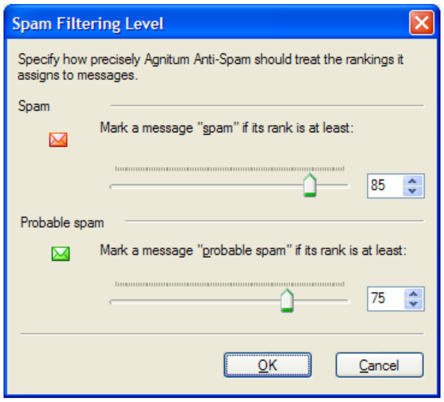
Normal

Optimal filtering level. Detects most of the spam messages with minimal false positives.

Filter training

☑ Train Anti-Spam on my outgoing e-mail also

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


Spam Filtering Level

Specify how precisely Agnitum Anti-Spam should treat the rankings it assigns to messages.

Spam

Mark a message "spam" if its rank is at least: 85

Probable spam

Mark a message "probable spam" if its rank is at least: 75

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

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

X-Agnitum-antispam: SPAM

X-Agnitum-antispam-rank: 99

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

4.8.5 Specifying White and Black Lists

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

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

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

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

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

The configuration and editing of both lists is similar. To add a new rule, click **Add**. In the **Edit Rule** window, you can specify the rule's parameters and conditions by following these steps:

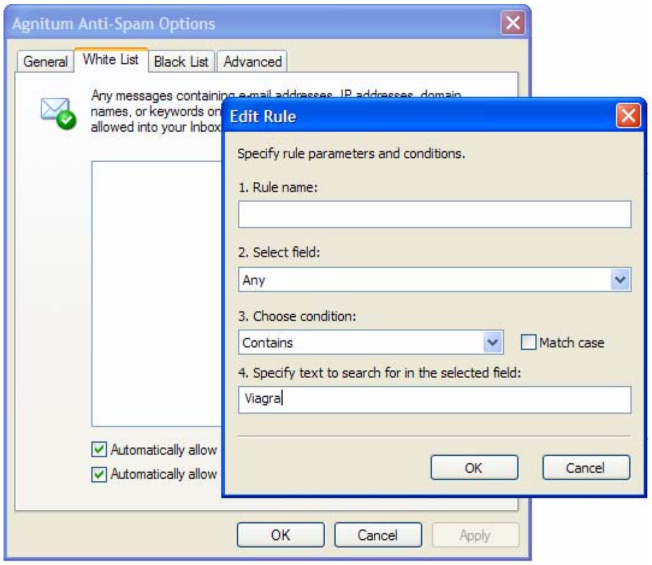
1. **Rule name.** Specify the rule name that will be displayed in the list. If you leave the text box blank, the name will be calculated automatically based on the rules parameters. The rule name does not affect the action of the filter.
2. **Select field.** Use the **Choose field** drop-down list to specify the field of the message to be searched. The following fields are available:

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

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

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

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



Specify rule parameters and conditions.

1. Rule name:

2. Select field: Any

3. Choose condition: Contains □ Match case

4. Specify text to search for in the selected field: Viagra

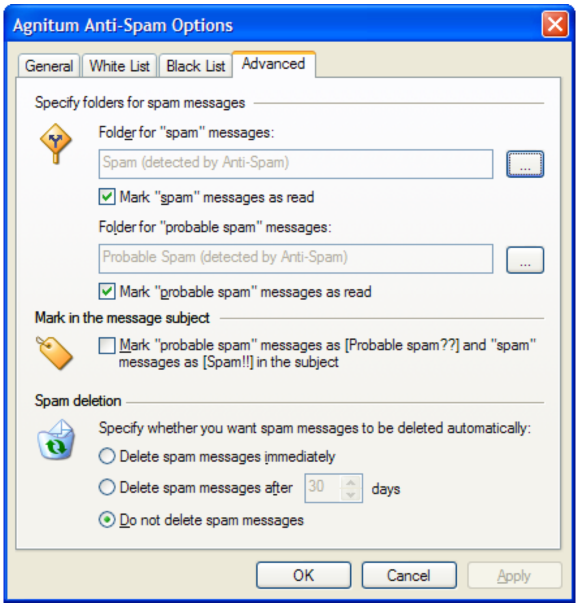
After specifying all the parameters, click **OK** to save the rule.

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

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

4.8.6 SPECIFYING ADDITIONAL SETTINGS

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



Specify folders for spam messages

Folder for "spam" messages: Spam (detected by Anti-Spam)

☑ Mark "spam" messages as read

Folder for "probable spam" messages: Probable Spam (detected by Anti-Spam)

☑ Mark "probable spam" messages as read

Mark in the message subject

□ Mark "probable spam" messages as [Probable spam??] and "spam" messages as [Spam!!] in the subject

Spam deletion

Specify whether you want spam messages to be deleted automatically:

○ Delete spam messages immediately

○ Delete spam messages after 30 days

● Do not delete spam messages

Specifying folders

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

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

Marking the message subject

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

Spam deletion

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

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

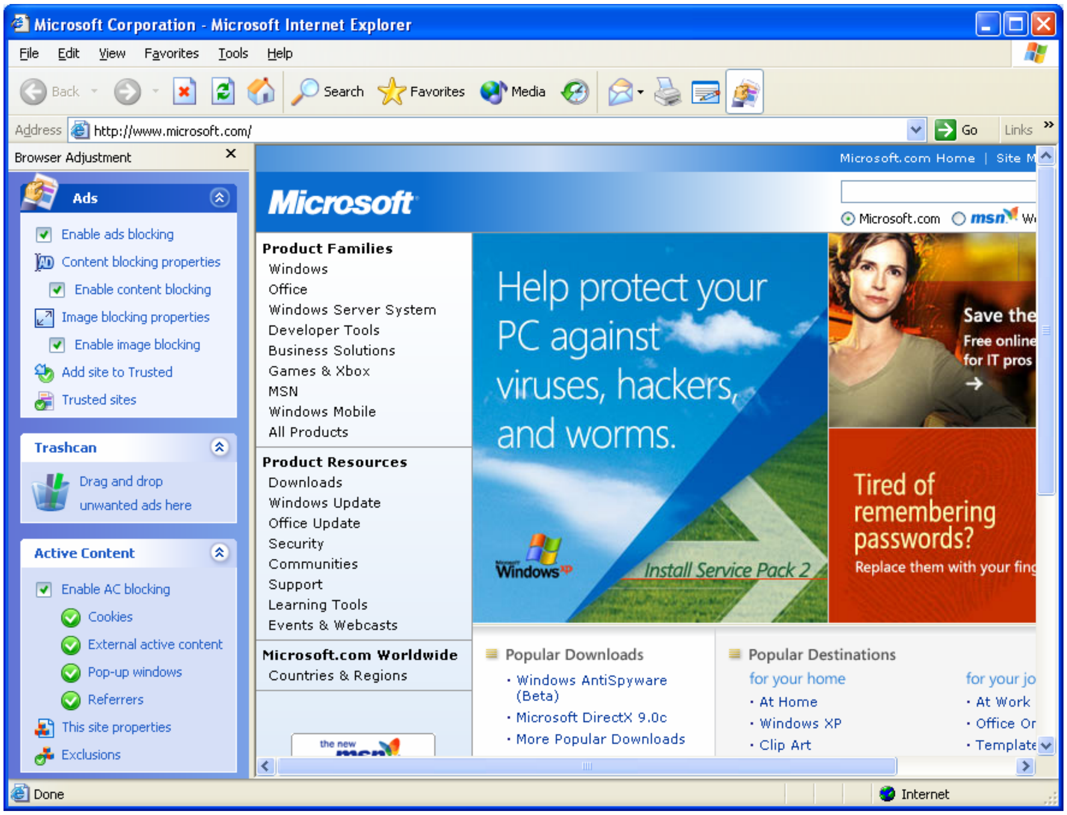
If you need time to periodically look through your spam folder in order to reveal false positives and are afraid of missing some useful information, select **Delete spam messages after ... days** and specify the number of days to keep spam. The aged spam will be deleted from the **Spam** folder after being kept the specified number of days.

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

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

4.9 Quick Tune

Outpost Security Suitevides the alternative way for controlling content of downloaded web pages directly from your browser. **Quick Tune** plug-in allows managing Ads and Active Content plug-ins settings using the special panel in Internet Explorer. To get access to the plug-ins settings from Internet Explorer, select **Explorer Bar > Outpost Security Suite Quick Tune** on the browser's **View** menu. The following panel will be displayed in the explorer bar:



Browser Adjustment

Ads
- ☑ Enable ads blocking
- Content blocking properties
- ☑ Enable content blocking
- Image blocking properties
- ☑ Enable image blocking
- Add site to Trusted
- Trusted sites

Trashcan
- Drag and drop unwanted ads here

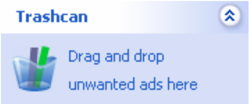
Active Content
- ☑ Enable AC blocking
- ✓ Cookies
- ✓ External active content
- ✓ Pop-up windows
- ✓ Referrers
- This site properties
- Exclusions

The panel contains sections with Ads and Active Content plug-ins settings which are similar to those displayed in the Outpost Security Suite interface. To enable/disable the blocking of ads/active content in your browser, click **Enable ads blocking/Enable AC blocking**.

Clicking the corresponding links in the panel you can open the plug-in properties and specify the settings the same way it is described above for each of the plug-ins.

Right-click the Quick Tune panel and click **Adjust Controlling Parameters** to select which active content elements you want to be displayed in the panel.

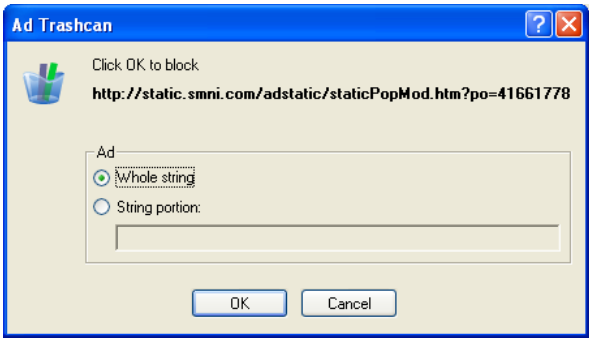
You can take an advantage of ad **Trashcan**. This small window makes it easy for you to remove an ad from a web page you are viewing, by simply dragging the ad over to the specified area.



Trashcan

Drag and drop unwanted ads here

Doing this will give you the following dialog:



Ad Trashcan

Click OK to block

http://static.smni.com/adstatic/staticPopMod.htm?po=41661778

Ad

● Whole string

○ String portion:

Select **String portion** if you want to trim the URL down. Then click **OK** to save the ad's URL into **Outpost Security Suite** base.

Note: To disable the plug-in, clear the **Explorer Bar** > **Outpost Security Suite Quick Tune** checkmark on the browser's **View** menu.

Part 2: For Advanced Users Only

5 Advanced Settings

5.1 Introduction

Our engineers configured **Outpost Security Suite's** default settings to give optimum protection for most computer systems and networks. **Outpost Security Suite** was designed from the start to be effectively used in its pre-configured state even by computer novices who need not know about network protocols to have their computer system safeguarded against malicious applications or web sites.

However, we also wanted **Outpost Security Suite** to be fully configurable to advanced users, those individuals who understand networking technology.

This chapter is provided so advanced users can effectively tweak **Outpost Security Suite** and learn about its most powerful features.

Note: A good rule of thumb when using **Outpost Security Suite** is to keep the settings **Outpost Security Suite** suggests if you do not have a particular reason and the knowledge to change them.

5.2 Saving and Loading Configurations

Outpost Security Suite has very many settings. Being able to save several different configurations of these settings lets you:

- Create different configurations for you and your family or colleagues.
- Prevent your children from accessing unwanted sites (sex, games, bomb making), from playing online games or chatting.
- Switch, using one mouse click, between "Work", "Rest", "I am away", "Block Everything", and "Children" configurations.
- Back up your configurations.

A configuration is the state **Outpost Security Suite** is in at any time. To create a new configuration, just change whatever settings you want and then go to the **File** menu (it is recommended to save your current configuration prior to this), select **Save Configuration As** and then enter the name you want to give that configuration. The **File** menu command **New Configuration** allows you to create a new configuration.

The default configuration file **Outpost Security Suite** uses is named **configuration.cfg**, located in the **Outpost Security Suite** installation folder. You can create several different configuration files simply by giving each a different name.

A configuration file can be protected by password. To do this, use the **Options** menu and select **General** then click **Enable** in the **Password protection** area of the dialog.

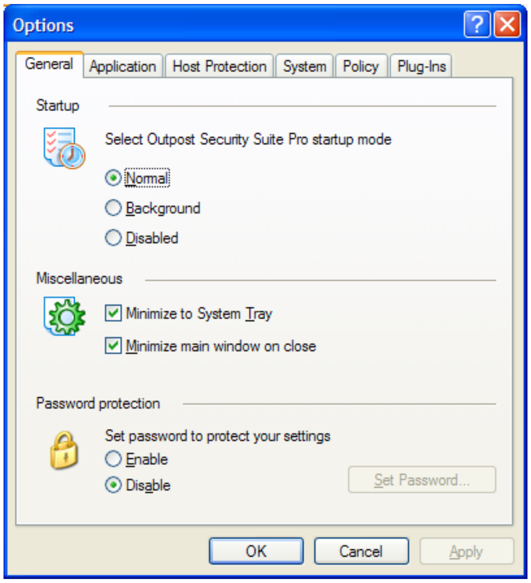
To change to a new configuration, use the **File** menu, select **Load Configuration** and choose the configuration file you want or simply select the configuration name on the **File** menu between **Save Configuration As** and **Exit**.

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

5.3 Setting a Password

You can safeguard the settings you give **Outpost Security Suite** by selecting a password. This will prevent all the data you entered into **Outpost Security Suite** from being changed. You can, for example, block access to objectionable sites for your children and know that your settings cannot be tampered with.

To set a password or change an old one, right-click the icon in the system tray, then select **Options**. You will see this dialog:



Startup

Select Outpost Security Suite Pro startup mode

● Normal

○ Background

○ Disabled

Miscellaneous

☑ Minimize to System Tray

☑ Minimize main window on close

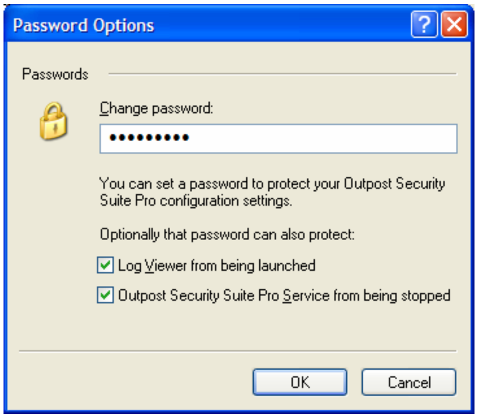
Password protection

Set password to protect your settings

○ Enable

● Disable

Select **Enable** under **Set password to protect your settings**. This brings up a small window in which you can enter the password you want. When you have entered in your password, click the **OK** button, then click the **Set Password** button in the above dialog window.



Passwords

Change password:
•••••••••

You can set a password to protect your Outpost Security Suite Pro configuration settings.

Optionally that password can also protect:

☑ Log Viewer from being launched

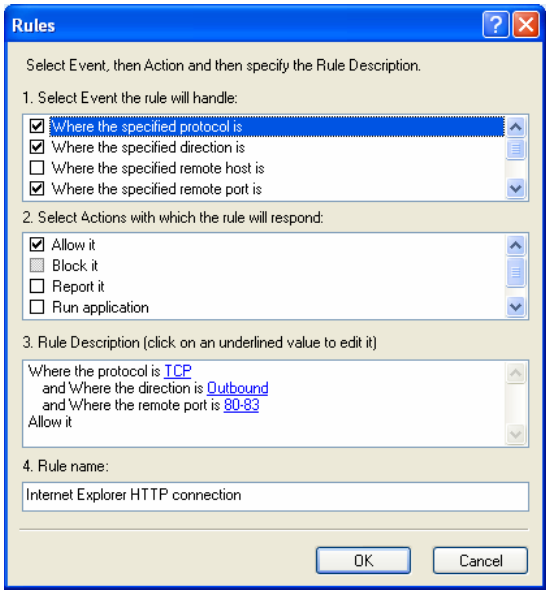
☑ Outpost Security Suite Pro Service from being stopped

By default, your password protects only your configuration settings from being altered, but you can additionally select to protect the Log Viewer and **Outpost Security Suite** service if you need to keep the system network history from being viewed by unauthorized persons or want to prevent them from unloading **Outpost Security Suite** and disabling its protection and the restrictions you set. This is most useful for parents who want to control their children and employers who need to restrict the activities of their employees.

Note: Remember your password!

5.4 Creating Rules for Applications

This section is an extension of what was covered earlier in 3.5 Application Level Filtering. The rules for applications can be set using the **Rules** dialog window. In the **Options** dialog, select the **Application** tab, highlight an application on the list, and select **Modify Rules** on the **Edit** menu. Click **New** to open the following dialog:



Select Event, then Action and then specify the Rule Description.

1. Select Event the rule will handle:

☑ Where the specified protocol is
☑ Where the specified direction is
☐ Where the specified remote host is
☑ Where the specified remote port is

2. Select Actions with which the rule will respond:

☑ Allow it
☐ Block it
☐ Report it
☐ Run application

3. Rule Description (click on an underlined value to edit it)

Where the protocol is TCP
  and Where the direction is Outbound
  and Where the remote port is 80-83
Allow it

4. Rule name:

Internet Explorer HTTP connection

Use of this dialog is recommended only for people who know about networking protocols.

First, describe the event to which the rule applies. You can select from the following criteria for your rule in the **Select Event this rule will handle** box:

- Where the specified protocol is
- Where the specified direction is
- Where the specified remote host is
- Where the specified remote port is
- Where the specified local port is
- Where the specified time interval is
- Where local port is equal to remote port

Selecting a check box adds its message to the **Rules Description** field. If a rule is listed as *undefined*, you should click it and select one of its options.

After describing the event, select an action for your rule in the **Select Actions with which the rule will respond** box. It can be:

- Allow it—Allows this communication.
- Block it—Blocks the communication. The source is not notified so it appears that the packet never arrived at the destination.
- Report it—Displays a message box when a rule is triggered.
- Run application—Runs the specified application with any specified command line parameters when a rule is triggered.
- Do not log this activity—disables activity logging for this rule. If selected, no data will be written to log on this rule triggering.
- Stateful Inspection—turns on “stateful inspection” for this application. If activated after an application connects to a remote server, all incoming communications from that server to the port opened by the application will be allowed.
- Ignore Component Control—forces Outpost to ignore Component Control during this communication if all the specified conditions are met.

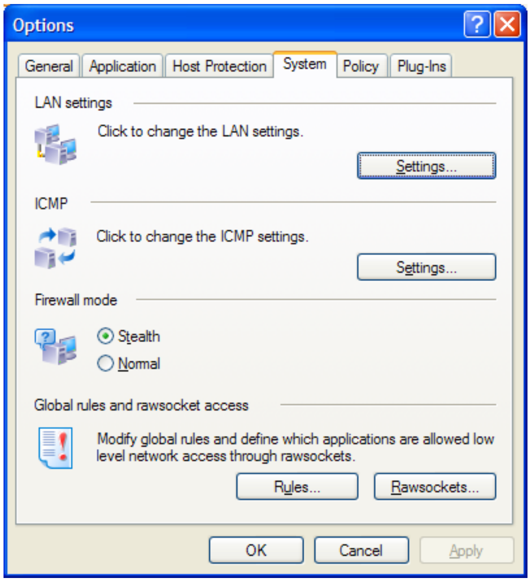
The final step is to assign a name to the rule. We recommend that you give a recognizable name to the rule, so it will be easy for you or others to understand it in the future. In addition, the name you give your rule appears in the **Allowed** or **Blocked** log as the **Reason** for allowing or blocking this communication. Outpost Security Suite suggests the name for the rule based on the specified settings.

It is prudent to save the present configuration before making changes to it.

Note: When an application tries to go online **Outpost Security Suite** checks if there are any rules for that application in the **Application Rules** list and, if so, **Outpost** uses those rules and ignores the Global Application and System Rules. Otherwise, **Outpost Security Suite** checks for rules matching the activity of the application in the **Global Application and System Rules** list and uses any that might apply.

5.5 System Level Filtering

Open the **Options** dialog window and select the **System** tab:



Click to change the LAN settings.

Click to change the ICMP settings.

● Stealth
○ Normal

Modify global rules and define which applications are allowed low level network access through rawsockets.

Note: These settings are for advanced users only. If any are incorrectly changed for your system or network, it could result in your firewall not working as expected.

The following options are available:

- **LAN settings—**lets you change the settings for your local area network, your NetBIOS choices, and lets you add or remove trusted IP ranges. **NetBIOS** is what Windows uses as the protocol for transferring shared files between computers and/or printers on a network. NetBIOS is useful on a LAN with trusted computers **but it can leave your computer open to attack if it is allowed for general Internet connections**. To learn more about configuring your LAN settings, refer to 5.6 Settings for a Home or Office Network.

- **ICMP—**lets you specify the types and directions of the ICMP messages allowed. The different types of ICMP messages are listed in Appendix B: Types of ICMP Messages. *It is recommended that you do not change the ICMP settings unless you are certain that you are making the right changes.* The **Default** button on the ICMP settings dialog resets all the ICMP settings to what they were when **Outpost Security Suite** was first installed.

- **Firewall mode—**to switch **stealth mode** on or off. Normally, when your computer receives a connection request from another computer it lets the other computer know that this port is closed. In **stealth mode,** your computer will not respond, making it seem like it is not turned on or not connected to the Internet. It is recommended that you keep **Outpost Security Suite** in **stealth mode** unless you have a reason not to.

- **Global rules and rawsocket access—**lets you specify global rules for all applications. Click **Rules** to edit the existing rules or to create new ones. The way the rules are created is similar to how application based rules are created. For details, see 5.4 Creating Rules for Applications.

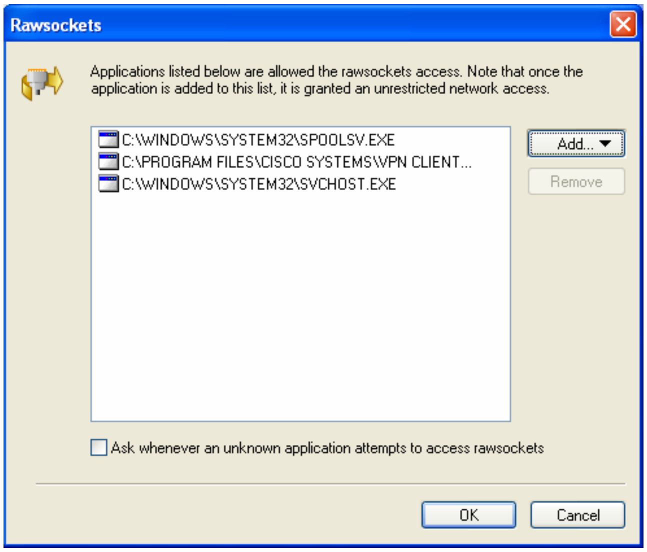
  The only differences are as follows.

  You can specify the packet type for outbound connections (i.e. when **Where the specified direction is** is **Outbound**:

  - **Local** packets from or to the local network interface
  - **Transit** packets that are passed along the system network interface or are forwarded to other interfaces (packets that are received and then sent further)
  - **NAT** packets – packets with translated IP-addresses (transit packets sent or received through a NAT proxy)

  Besides, you can mark the rule as a **High Priority** if you want this rule to prevail over the application rules which take precedence by default.

  Some applications can also access the network through direct low-level socket calls, also known as rawsockets. These calls cannot be governed by ordinary protocols or application rules and thus can serve as backdoors for rogue applications or processes to access the network without any limits or regulations. To improve your system protection, **Outpost Security Suite** lets you control rawsocket access. You can define which applications are allowed to make rawsocket calls and which are not. Click **Rawsockets** to bring up the following dialog:



Applications listed below are allowed the rawsockets access. Note that once the application is added to this list, it is granted an unrestricted network access.

C:\WINDOWS\SYSTEM32\SPOOLSV.EXE
C:\PROGRAM FILES\CISCO SYSTEMS\VPN CLIENT...
C:\WINDOWS\SYSTEM32\SVCHOST.EXE

□ Ask whenever an unknown application attempts to access rawsockets

  Click **Add** and select the application that you want to grant rawsocket access. If you want **Outpost Security Suite** to ask you each time an application that is not on the allowed list attempts to access rawsockets, select the corresponding check box.

5.6 Using Macro Addresses

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

Outpost Security Suite 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.

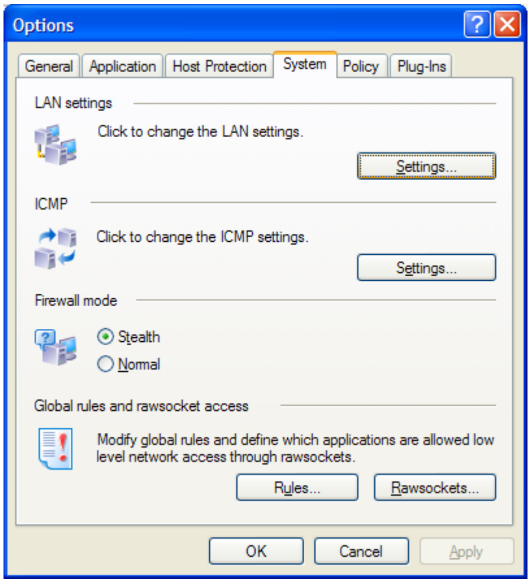
When you specify a local or remote address, you can select one of the following macros:

- **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”.

5.7 Settings for a Home or Office Network

A fundamental difference between a local area network (LAN) and the Internet is the level of trust you can grant them. A LAN, used in the home or an office, is generally comprised of “friendly” computers—computers belonging to or operated by other family members or fellow workers. A LAN can be called a **Trusted Zone**.

To check or reconfigure your network settings, right-click **Outpost Security Suite’s** icon in the system tray and select **Options**. Select the **System** tab to get the following dialog:



LAN settings

Click to change the LAN settings.

ICMP

Click to change the ICMP settings.

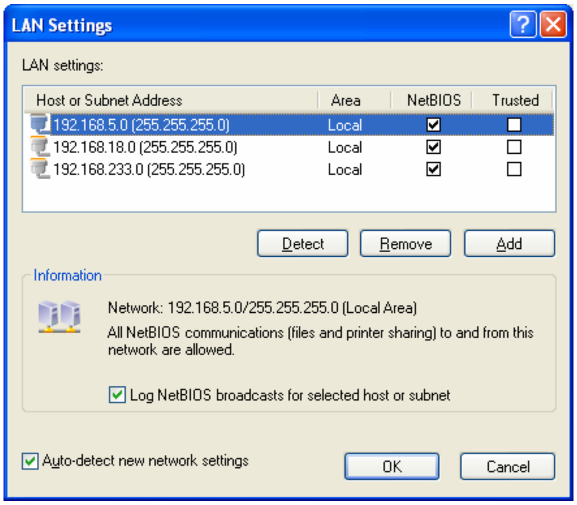
Firewall mode

● Stealth
○ Normal

Global rules and rawsocket access

Modify global rules and define which applications are allowed low level network access through rawsockets.

In the **LAN Settings** section, click the **Settings** button to display the **LAN Settings** window:



LAN settings:

Host or Subnet Address	Area	NetBIOS	Trusted
192.168.5.0 (255.255.255.0)	Local	☑	□
192.168.18.0 (255.255.255.0)	Local	☑	□
192.168.233.0 (255.255.255.0)	Local	☑	□

Information

Network: 192.168.5.0/255.255.255.0 (Local Area)

All NetBIOS communications (files and printer sharing) to and from this network are allowed.

☑ Log NetBIOS broadcasts for selected host or subnet

☑ Auto-detect new network settings

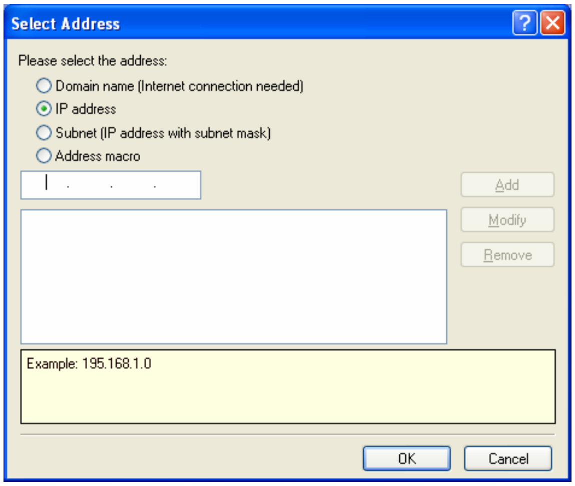
Normally when you open this window you will see your network address, but if you selected the **Configuration Wizard** during the **Outpost Security Suite** installation process and removed all detected networks, then this window will most likely be blank. To detect your network automatically, click the **Detect** button.

It is also recommended that you keep **Auto-detect new network settings** selected for **Outpost Security Suite** to automatically detect any new networks so you will not have to add them manually.

If you wish to allow all connections for a particular network, select the corresponding check box in the **Trusted** column**.** Otherwise, if you want to remove the network address from the **Trusted Zone**, clear the check box.

If you want to allow all NetBIOS communications—to and from a network address—make sure the corresponding box in the **NetBIOS** column is selected. To disallow all communications with the network, just clear the **NetBIOS** and **Trusted** check boxes.

You can also add a custom remote network address to Trusted Zone. Click the **Add** button to display the following dialog window:



Select Address

Please select the address:

○ Domain name (Internet connection needed)
● IP address
○ Subnet (IP address with subnet mask)
○ Address macro

Example: 195.168.1.0

Specify the domain name, IP address, or IP range. An example is given below the selection area for each type of address designation. An active Internet connection is required for **Domain name (Internet connection needed)** because the IP address needs to be looked up directly over the Internet. The IP address is saved along with the domain name you enter and this is the IP address that is mostly used by **Outpost Security Suite**.

Click the **Add** button to add a new entry to **Outpost Security Suite's** Trusted Zone listing.

An entry on the trusted list can be modified at any time by highlighting it, amending it, and clicking the **Modify** button.

To remove an entry, highlight it on the list and click the **Remove** button.

Please note that plug-ins are independent from the Trusted Zone settings. For example, even if we add www.agnitum.com to the trusted network addresses, **Outpost Security Suite** plug-ins will block banners, active content and other things from this site regardless.

In addition, it is very important to remember that Trusted Zone rules are given the highest priority possible. Even restricted applications can communicate with Trusted Zone hosts. *We advise you to put ONLY your absolutely trusted computers into this zone.* If you only need file and printer sharing, it is best to use **NetBIOS** rather than **Trusted**.

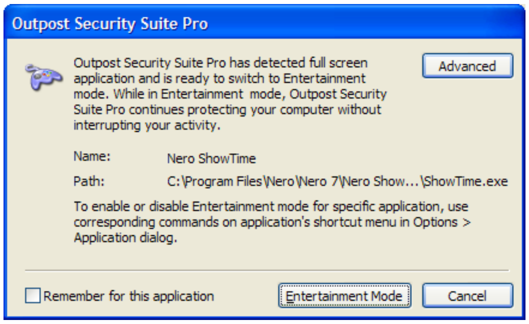
Note: If you do not want to clutter up logs with information about NetBIOS broadcast packets, you can specify to disable these data logging for each of the detected host or subnet. Select the address from the list and clear the **Log NetBIOS broadcasts for**

selected host or subnet check box in the **Information** area. This will keep Log Viewer data more clear and may improve computer performance.

5.8 Running in Entertainment Mode

When playing games or watching movies you probably want to avoid product prompts and alerts from distracting your attention or capturing focus, yet still want to be protected, especially when playing online.

Outpost Security Suite provides a specially designed **Entertainment mode** where protection is active without bothering users with numerous product prompts and alerts. Once the full screen application (a game, media player, etc.) is started, Outpost Security Suite detects this event and suggests entering Entertainment mode, so the application runs using the background/Entertainment mode policy that is specified in **Options** > **Policy** > **Advanced** dialog, in which case no alerts and messages are displayed with the full screen application and updates are not checked.



Outpost Security Suite Pro

Outpost Security Suite Pro has detected full screen application and is ready to switch to Entertainment mode. While in Entertainment mode, Outpost Security Suite Pro continues protecting your computer without interrupting your activity.

Name: Nero ShowTime

Path: C:\Program Files\Nero\Nero 7\Nero Show...\ShowTime.exe

To enable or disable Entertainment mode for specific application, use corresponding commands on application's shortcut menu in Options > Application dialog.

If you want a particular application to always or never use Entertainment mode, select the **Remember for this application** check box before responding to the dialog box. You can also enable or disable Entertainment mode for specific applications in the **Options** > **Application** list using the commands on the application's shortcut menu. Select **Entertainment Mode** > **Enable Entertainment Mode** or **Disable Entertainment Mode** for Outpost Security Suite to automatically change its policy when the application enters full screen mode.

To configure specific Entertainment mode settings, click **Advanced**. The displayed window lets you set the rules that will be used by Outpost Security Suite whenever you enter Entertainment mode, and lets you define whether advanced protection techniques such as Component Control, Anti-Leak Control and real-time malware protection should be enabled while Outpost Security Suite runs in Entertainment mode.

Note: When operating in background mode, Outpost Security Suite does not enter Entertainment mode.

Note: When an application—with no network access rules already set—enters Entertainment mode, it is put in the **Trusted applications** group.

5.9 Running in Self-Protection Mode

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

By default, self-protection is enabled. To disable it, click the **Self-Protection** button on the toolbar.

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.

6 The Outpost Log System

6.1 Introduction

Outpost Security Suite performs many different functions as it protects your computer from attacks. Each action it takes is referred to as an event and every event is logged.

To make it easy for you to view these event logs our engineers created the **Outpost Log Viewer**. This shows you the history of every operation **Outpost Security Suite** performed including:

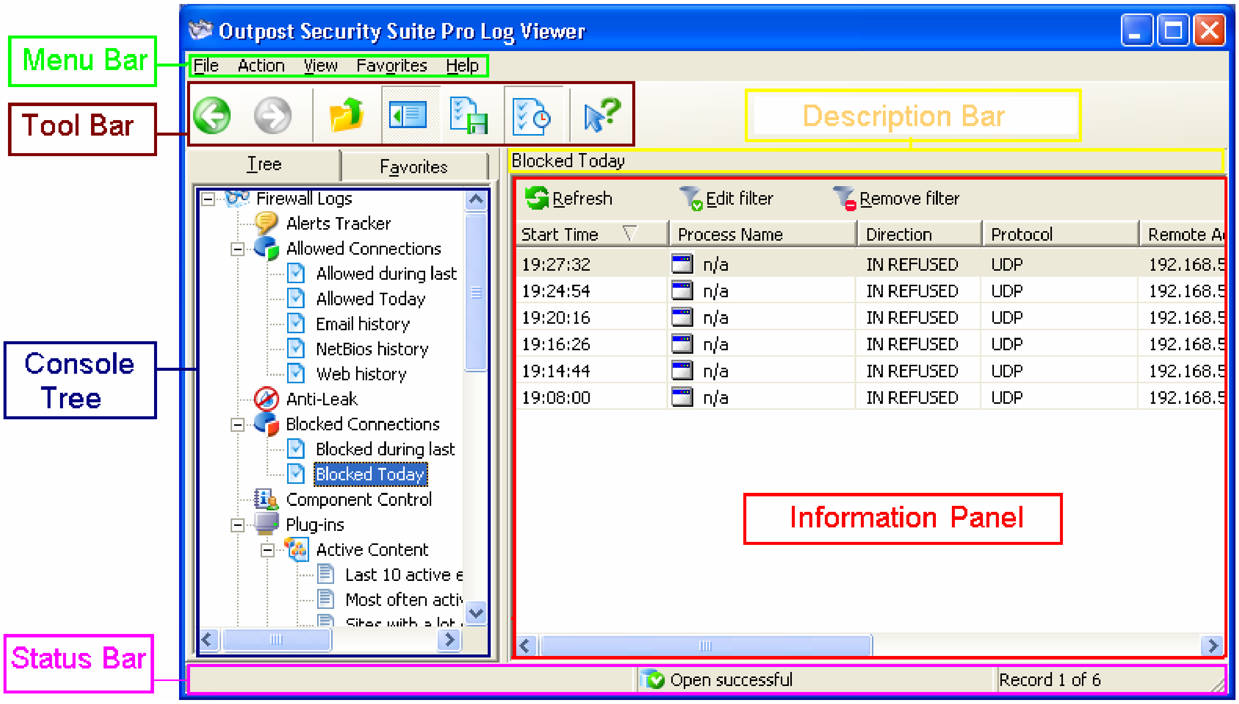
- Every application and connection that was allowed or blocked by **Outpost Security Suite**.
- The specific activities of each **Outpost Security Suite** plug-in.
- The start of every program and all changes made to policies, configuration settings and passwords.

The main features of the **Outpost Log Viewer** are:

- One mouse click to view the entire log or a selection of specific events. See the 6.3 How to Display Logs chapter for details.
- Customized display of the logs. You can view only the information you need by selecting columns and limiting their parameters and sorting by any parameter.
- Preset selections of events can be displayed. You can easily switch between connections blocked during the last ten minutes, for instance, or all connections allowed today. You can also create, edit and remove selections of events to be displayed. See the 6.4 Working with Logs and Filters chapter for details.
- Filters can be added to organize the data displayed.
- Logs can be copied and/or exported according to presets, filters or selected records.
- Log files can be cleared to save hard drive space.
- Customized SQL queries can be created for specific monitoring purposes.
- Logs can even be browsed via the Microsoft Management Console (MMC) snap-in.
- Logging can be disabled by clearing the **Tools** > **Enable Logging** check box from the Outpost main window.

6.2 Outpost Log Viewer's Main Window

The main window of the Outpost Log Viewer allows you to view and work with the logs. To access this window select **Tools** from **Outpost Security Suite's** menu and then select **Outpost Log Viewer.** This is how the window looks:



Blocked Today

Start Time	Process Name	Direction	Protocol	Remote A
19:27:32	n/a	IN REFUSED	UDP	192.168.5
19:24:54	n/a	IN REFUSED	UDP	192.168.5
19:20:16	n/a	IN REFUSED	UDP	192.168.5
19:16:26	n/a	IN REFUSED	UDP	192.168.5
19:14:44	n/a	IN REFUSED	UDP	192.168.5
19:08:00	n/a	IN REFUSED	UDP	192.168.5

Open successful   Record 1 of 6

The main elements of Outpost Log Viewer are:

- The Menu Bar.
- Console Tree
- Information Panel
- Tool Bar
- Description Bar
- Status Bar

The console tree and information panel are similar to the left and right panels of Windows Explorer. The console tree is a listing of the filters and the information panel gives detailed data about whatever filter is highlighted in the console tree.

As with Windows Explorer, any line that starts with a plus sign (+) can be expanded to show each of its subcategories. Any line starting with a minus sign (-) shows that the line has already been expanded. By clicking on the minus sign, all of its subcomponents can be hidden so only the name of the component is displayed to conserve screen space.

To expand or collapse all the items of a log or plug-in:

1. In the console tree, right-click a log or plug-in.
2. Select **Expand All** or **Collapse All** on the shortcut menu.

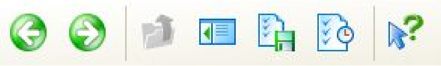
The console tree consists of two tabs: **Tree** and **Favorites**. For more information about **Favorites**, see the 6.5 Working with Favorites chapter for details.

On the **Tree** tab, there are the following groups of logs:

- **Alerts Tracker**
  A listing of all the displayed notifications.
- **Allowed Connections**
  A listing of every application and connection that **Outpost Security Suite** allowed.
- **Anti-Leak**
  Displays all the Anti-Leak Control activity events.
- **Blocked Connections**
  A listing of every application and connection that **Outpost Security Suite** blocked.
- **Component Control**
  Displays all the Component Control activity events.
- **Plug-Ins**
  Each plug-in has its own log:
  - **Active Content** displays the sites that had some of its active content blocked based on the settings for Java applets, JavaScript, VBScript, ActiveX objects and other active content elements.
  - **Ads** displays a list of all the ads that were blocked.
  - **Anti-Malware** displays a list of all spyware objects detected in your system and the actions performed.
  - **Attack Detection** shows every suspicious activity and attack on your computer from the Internet, the ports involved and where the attacks originated.
  - **Content** lists all the web sites or pages that were blocked due to their content.
  - **DNS Cache** displays the web addresses saved by Outpost Security Suite to speed up your Internet connection to those sites.
- **System Log**
  This is a record of every program start and every change made to the firewall policies, program options and configuration settings.

The information is arranged in a table. The columns of this table represent the various log parameters, such as **Application**, **Start Time**, **Protocol**. Each log has its own set of parameters. See the 6.3 How to Display Logs chapter for details.

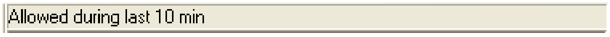
The Outpost Log Viewer toolbar is near the top of the main window and looks like this when **Outpost Security Suite** is first installed:



When working with Outpost Log Viewer, you can see a tooltip explaining what each button does by holding your cursor over it for a second or so. Here is what each button does:

Button	Function
←	Goes back to the previous viewed item.
→	Goes forward to the next viewed item.
↑	Goes up one level.
▤	Shows or hides the console tree.
💾	Exports the selected log.
🕒	Enables log auto refresh.
?	Displays context help.

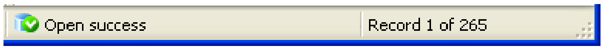
The description bar is right above the information panel in the Outpost Log Viewer window and looks like this:



Allowed during last 10 min

It displays a description of the filter selected in the console tree.

The status bar is at the bottom of the Outpost Log Viewer window and looks like this:



Open success

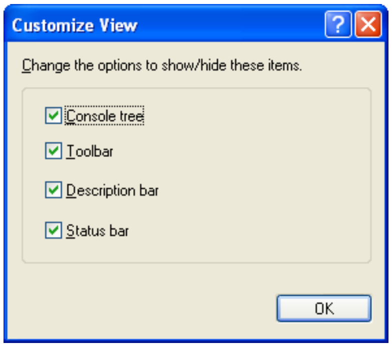
Record 1 of 265

It consists of two sections that display the following information:

- The result of attempting to open the selected log.
- The number of the record being viewed and the total number of records in that log.

You can locate data more comfortably by showing or hiding specific parts of the Outpost Log Viewer window. To customize the Log Viewer's layout, select **Layout** on the **View** menu.

You will see the **Customize View** dialog, which looks like this:



Change the options to show/hide these items.

☑ Console tree

☑ Toolbar

☑ Description bar

☑ Status bar

Select the elements you want to display and clear those you want to hide.

To show or hide the console tree, you can also use the ◧ button on the Outpost Viewer toolbar.

6.3 How to Display Logs

To view Outpost Security Suite's logs, select **Tools** from **Outpost Security Suite**'s menu, then select **Outpost Log Viewer**. Select the items of interest in the console tree as described below or switch to the **Favorites** tab (see the 6.5 Working with Favorites chapter for details).

You can also open the specific Log Viewer entry you are interested in directly from the main Outpost's window. To do so, perform the following actions:

1. In the left panel of the main window, select the component you want to view the statistics for.
2. Click the **Show Detailed Log** button on the information panel if you want to see the entire log or select a preset or filter from the menu using the **Show Log Preset** button.

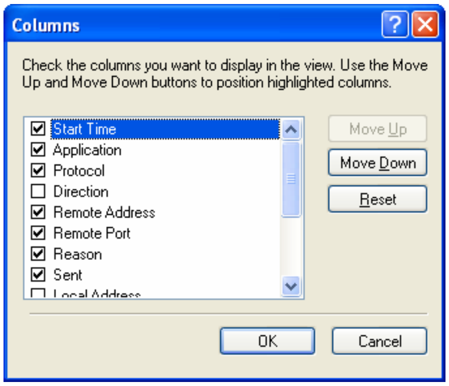
The Outpost Log Viewer will be opened showing the details of the log.

Content in the Outpost Log Viewer changes quickly so to display the latest data in the information panel, don't forget to refresh it occasionally by highlighting the log, preset or filter you want to refresh in the console tree and clicking the **Refresh** button in the information panel.

The history of **Outpost Security Suite**'s activity is displayed in Log Viewer's information panel as a table. Every log has its own set of columns. You can configure Log Viewer to show only the columns you are interested in and in any sequence.

To select the columns you want displayed for the selected log, right-click anywhere in the information panel and select **Columns** from the shortcut menu**.** Alternatively, you could select **Add/Remove Columns** on the **View** menu**.**

You will see the **Columns** dialog that looks like this:



Columns

Check the columns you want to display in the view. Use the Move Up and Move Down buttons to position highlighted columns.

- ☑ Start Time
- ☑ Application
- ☑ Protocol
- □ Direction
- ☑ Remote Address
- ☑ Remote Port
- ☑ Reason
- ☑ Sent
- □ Local Address

Select the columns you want to be displayed in the information panel.

To change the sequence of columns in your log, use the **Move Up** or **Move Down** buttons. This can also be done directly from the main Log Viewer's window by simply dragging the columns in the information panel (by holding the left mouse button down) to arrange them in whatever order you want. To revert to the default order, click **Reset**.

To resize a column, point to the caption of the columns and position the cursor over its border, the cursor changes to a double-headed arrow. Click the left mouse button and keep it pressed while moving the cursor. Release the button as soon as the column has reached the size you want.

Outpost Log Viewer also lets you sort the records of a log by the values of any column in descending or ascending order. Click the header of the column you would like to use to sort the records. If the header shows an arrow pointing upwards , the records will be sorted in ascending order (i.e. 1, 2, 3…). To reverse the order, just click again. The header now shows a downward arrow and the records will be in descending order (i.e. 3, 2, 1).

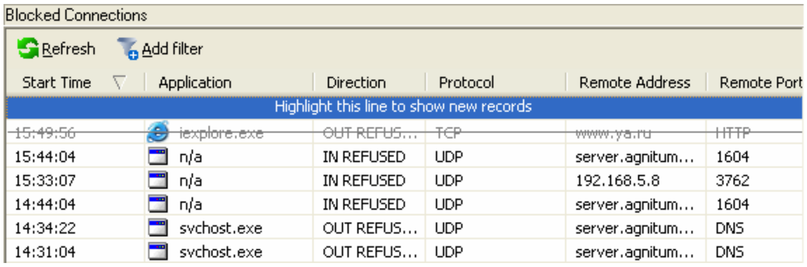
To make it easier to locate specific data in a log, you can show or hide records containing the same data in any of displayed columns. Select the corresponding record in the information panel. Right-click the cell that contains the data of interest and select **Include Selection** from the shortcut menu to show the records with similar data or **Exclude Selection** to hide them. If there are other cells that have the same data for several records, you can add that also. To show all the records again, select **Show All** from the shortcut menu.

Example: To view data on connections established by a certain application at a particular time, select the **Allowed Connections** log, right-click the cell with record containing information on the application in the **Application** column and select **Include Selection**. Then right-click the **Start Time** column on the required date and time and select **Include Selection** again. The information panel will now display all the records of the selected date regarding the selected application.

This operation can be done so quickly that there is no reason to save the configuration. To create a permanent selection of records under complex conditions, create a filter.

Notes: Include Selection and **Exclude Selection** commands are not available for some logs.

While in the Rules Wizard mode, some particular records can be displayed in Outpost Security Suite Log Viewer. If Outpost Security Suite Log Viewer is open and some application requests the network access which is not described by any of the existing rules, the prompt is displayed and the application is blocked until the user takes the decision. Such an application will be displayed in the **Blocked Connections** log. If the user allows the network access, the records in this log are displayed as shown in the following picture:



Start Time	Application	Direction	Protocol	Remote Address	Remote Port
Highlight this line to show new records					
~~15:49:56~~	~~iexplore.exe~~	~~OUT REFUS...~~	~~TCP~~	~~www.ya.ru~~	~~HTTP~~
15:44:04	n/a	IN REFUSED	UDP	server.agnitum...	1604
15:33:07	n/a	IN REFUSED	UDP	192.168.5.8	3762
14:44:04	n/a	IN REFUSED	UDP	server.agnitum...	1604
14:34:22	svchost.exe	OUT REFUS...	UDP	server.agnitum...	DNS
14:31:04	svchost.exe	OUT REFUS...	UDP	server.agnitum...	DNS

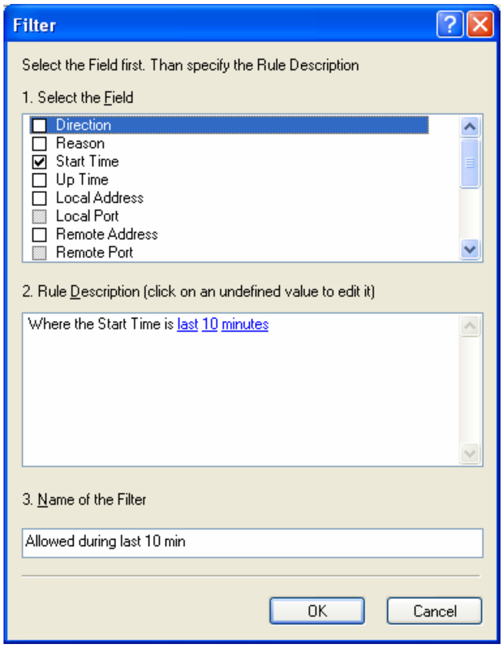
6.4 Working with Logs and Filters

There are several useful operations you can perform with logs:

- Creation of filters.
- Adding logs, filters or presets to **Favorites**.
- Copying logs, filters, presets or particular records to the Windows clipboard.
- Exporting logs, filters, presets or records to text files.
- Clearing logs.

A **filter** is a way of selecting out specific logged events; it filters out only the data you want from all the data contained in a log. A filter is named to show the data it presents and it appears as a separate item in the console tree. The conditions (rules) of filtering are specified by the user. The rules are based on each column (type of data) that is in a log. Filtering out only the data that you are interested in is a powerful and flexible feature. With filters, you can narrow your search to only the data within a specific time span and/or only the data about a particular application, port, etc.

To create a filter, click the **Add Filter** button in the information panel. This command is also available in Outpost Log Viewer's menu under **Actions** > **Add Filter** and in the shortcut menus of each log in the console tree. You will see the **Filter** dialog with a listing of the columns in that log:



Filter

Select the Field first. Than specify the Rule Description

1. Select the Field

- □ Direction
- □ Reason
- ☑ Start Time
- □ Up Time
- □ Local Address
- □ Local Port
- □ Remote Address
- □ Remote Port

2. Rule Description (click on an undefined value to edit it)

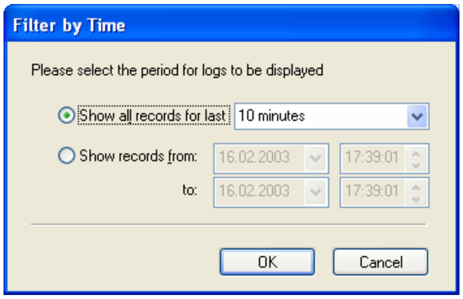
Where the Start Time is last 10 minutes

3. Name of the Filter

Allowed during last 10 min

To specify a filtering rule, select each column of data you want to see. In the description field, the beginning of the rule appears, such as: "Where the Start Time is Undefined".

To continue the rule, click Undefined. You will see a dialog in which you can specify various limitations for the selected column:



Filter by Time

Please select the period for logs to be displayed

● Show all records for last 10 minutes

○ Show records from: 16.02.2003 17:39:01

to: 16.02.2003 17:39:01

Use this dialog window to meet your needs and click **OK**. The rule will be completed according to the choice you have made. For example: "Where the Start Time is last 5 minutes."

You can specify as many rules as you like, then enter the filter name and click **OK**. The new filter will appear in the console tree.

You can also edit an existing filter by clicking the **Edit Filter** button in the information panel and editing all the settings of the filter as described above.

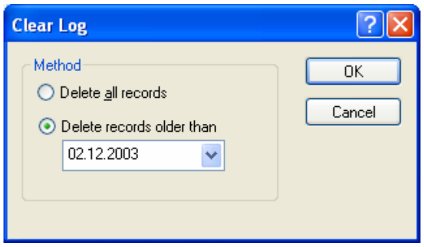
It is also possible to remove an unnecessary filter by highlighting it in the console tree and pressing the **Remove Filter** button. The filter will be removed from the console tree.

You can quickly view a filter from within the **Outpost Security Suite's** main window (see the 6.3 How to Display Logs chapter for details) or add it to **Favorites** (see the 6.5 Working with Favorites chapter for details).

To save specific logged data to a text or comma separated value file or copy it to the clipboard to paste it to other applications:

1. In the Log Viewer's console tree, select the log of interest.
2. Select the records you want to copy or export.
   - To select a group of records, click the first one and then press the **Shift** key while clicking on the last one.
   - To select separate records, click each while holding down the **Ctrl** key.
   - Use **Include Selection** or **Exclude Selection** in a record's shortcut menu (right-click a record to get the menu) to make an advanced selection by using one or several columns.
3. Right-click a selection and select **Export** or **Copy** from the shortcut menu.
4. Specify the folder to which the data will be exported and the file type and name. If you are copying records then remember to paste them into another file.
5. Click **OK**.

Logs are stored in a database that is compressed automatically to conserve space on your hard disk, so there is usually no need to clear these logs. However, you may want to clear them from your hard drive. In the console tree, select the log of interest and right-click in the information panel to display the shortcut menu. Select **Clear Log** to see the following dialog:



Clear Log

Method

○ Delete all records

● Delete records older than 02.12.2003

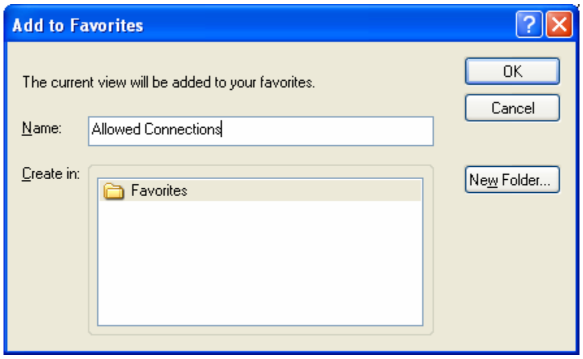
Select either **Delete all records** or specify the date of the last record to be deleted.

6.5 Working with Favorites

The console tree consists of two tabs: **Tree** and **Favorites**. **Favorites** is where you can keep things that you use often.

You can add logs, presets or filters that you frequently use to the **Favorites** tab for convenient and quick access. In the console tree, right-click the required item (group of logs, log, log preset or filter) and select **Add to Favorites**.

The **Add to Favorites** dialog will be displayed:



The current view will be added to your favorites.

Name: Allowed Connections

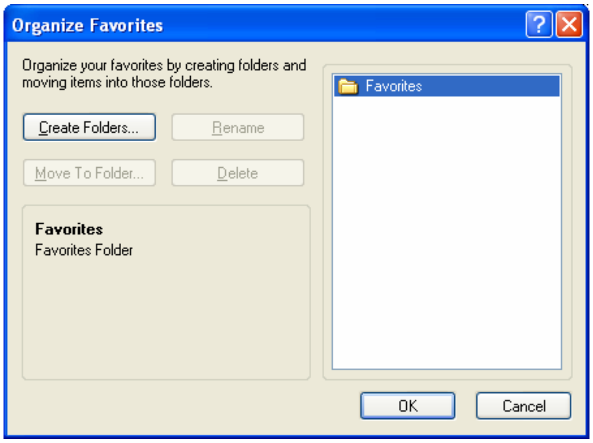
Create in: Favorites

If desired, rename the item in the **Name** edit field and select a folder to place it in or create a new one by clicking on the **New Folder** button. Click **OK**. The item appears on the **Favorites** tab in the specified folder.

To display the items you saved in **Favorites**, just click **Favorites** in the console tree and select the required item.

To delete items from **Favorites**, in the console tree, click the **Favorites** tab. Right-click the required item and select **Remove**.

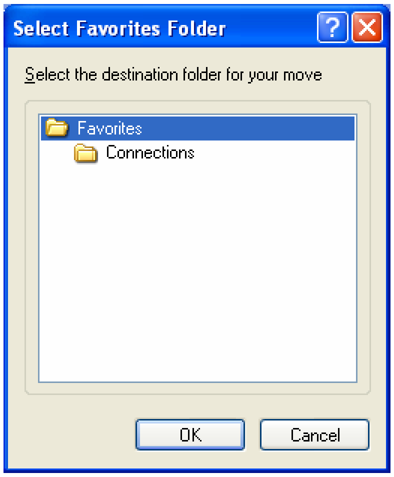
To rearrange the order of items in **Favorites**, select **Favorites** from the Log Viewer’s menu and select **Organize Favorites** to get this dialog:



Organize your favorites by creating folders and moving items into those folders.

Favorites
Favorites Folder

To create a new folder, click the **Create Folder** button. To rename or delete an item, select the item and click **Rename** or **Delete**. Clicking on **Move to Folder** displays the **Select Favorites Folder** dialog:

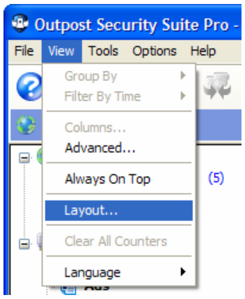


Highlight the folder you want the item to be moved to and click **OK**.

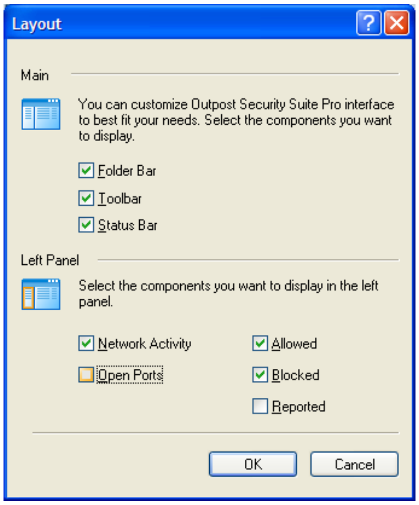
Appendix A: Customizing Outpost Main Window

Layout

You can choose not to display the folder bar, tool bar and the status bar in order to increase the amount of viewing space of the information panel. To do this, click the **View** menu and select **Layout** as shown here:



The following dialog box lets you clear check boxes next to these bars:



Layout

Main

You can customize Outpost Security Suite Pro interface to best fit your needs. Select the components you want to display.

☑ Folder Bar

☑ Toolbar

☑ Status Bar

Left Panel

Select the components you want to display in the left panel.

☑ Network Activity ☑ Allowed

☐ Open Ports ☑ Blocked

☐ Reported

OK Cancel

In the **Left panel** section are the categories that can be displayed or hidden in the left panel's listing by selecting or clearing them in this dialog. These are:

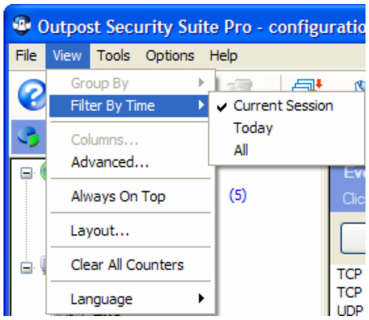
- **Network Activity**—all objects with a network activity.
- **Open Ports**—all objects with an open port for a network connection.
- **Allowed**—shows the events log for all applications with a protocol that is supported and allowed for network operation.
- **Blocked**—shows the events log for all applications with network connection attempts that were blocked.
- **Reported**—shows the events log for all applications for which a report on their network operations must be made according to **Outpost Security Suite's** settings.

Note: The same object can be in several lists as applicable.

Filter by time

This filters out the data displayed that you are not interested in. **Filter by time** limits the event log display to the **Allowed**, **Blocked** and **Reported** items of the left panel.

Filter by time is only available on the **View** menu when one of the left panel items **Allowed**, **Blocked** or **Reported** is highlighted as shown here**:**



An alternate way to access the **Filter by time** dialog window is from **Outpost Security Suite's** toolbar. The **Filter by time** button that is accessible only when one of the left panel's **Allowed**, **Blocked** or **Reported** items is highlighted.

Filter by time lets you choose from three options:

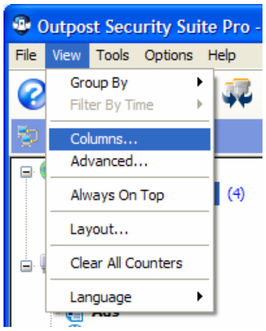
- **Current session—**shows the event log for the current session of Outpost Security Suite.
- **Today—**shows the event log for the current date.
- **All—**shows the entire event log from the time you started using Outpost.

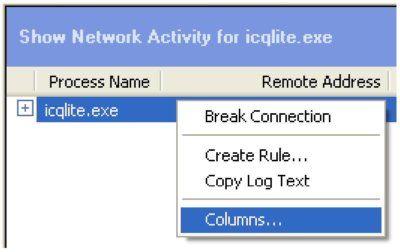
To find out how to filter Outpost Log Viewer logs, refer to 6 Outpost Log System chapter.

Columns

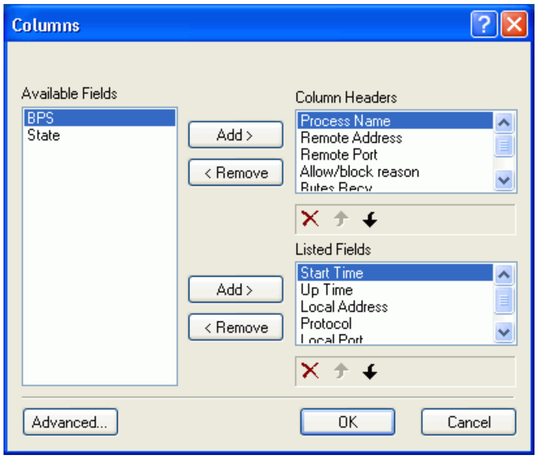
With the **View** menu's **Columns** option, you can configure **Outpost Security Suite** to show you only those data you are interested in. This is also available from the information panel element's shortcut menu.

Please note that the **Columns** menu is available for **Network Activity** and **Open Ports** items only.

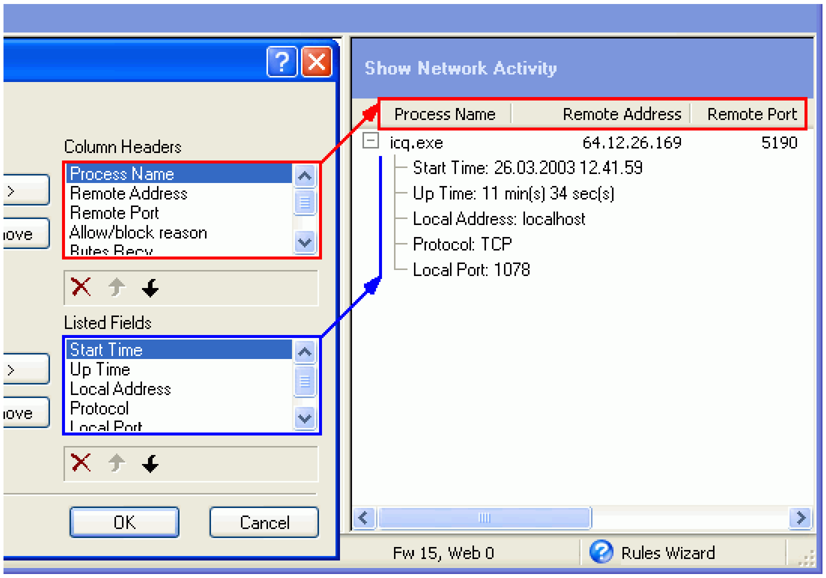




After clicking on the **Columns** option from the **View** menu the following dialog is displayed:



The **Column Headers** and **Listed Fields** in this dialog correspond to those in the information panel as shown here:

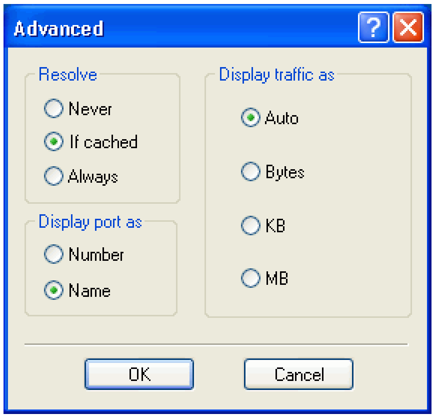


icq.exe 64.12.26.169 5190
Start Time: 26.03.2003 12.41.59
Up Time: 11 min(s) 34 sec(s)
Local Address: localhost
Protocol: TCP
Local Port: 1078

You can customize the listings by removing an item from the list using the **Remove or** ☒ button or adding a previously removed item back to the list using the **Add** button.

You can re-arrange the sequence of the items for each listing also. To move an item in either the **Listed Fields** or **Column Headers** list, use the up arrow button ↑ to move the item one line up or the down arrow button ↓ to move the item one line down. These buttons are located under the listing they affect.

The **Advanced** command on the **View** menu also allows you to customize the display of information in columns:



Advanced

Resolve
○ Never
● If cached
○ Always

Display port as
○ Number
● Name

Display traffic as
● Auto
○ Bytes
○ KB
○ MB

The **Resolve** section gives you the choice of displaying network addresses as DNS address (for example, www.agnitum.com)

- **Never**—always display these addresses as IP addresses (for example, 64.176.127.178).
- **If cached**—convert these to their DNS addresses if the information for the address conversion is stored in the DNS Cache module.
- **Always**—always convert and display these addresses as DNS addresses. **However, this is not recommended as it can result in a great number of DNS requests.**

The **Display port as** section lets you display the local port (on your computer) and **r**emote port values as:

- **Number**—ports are displayed as numbers.
- **Name**—ports are displayed as names describing their task, if the information is available in the system for that port (for example, “www” rather than “80”).

The **Display traffic as** section lets you specify the base measure of the amount of transferred information in the **Sent** and **Received** fields as:

- **Auto**—displays traffic in the most suitable measurement.
- **Bytes**—displays traffic in number of bytes sent or received.
- **KB**—displays traffic in kilobytes.
- **MB**—displays traffic in megabytes.

Group By

Group By is a very useful option on the **Outpost Security Suite's View** menu. Using it, you can get the information you need very quickly. Normally, the information is grouped by application, which is generally the most useful grouping of information. For example, you can select **Group By Application**, then click the application you are investigating in the left panel and **Outpost Security Suite** lists all the connections of this particular application and nothing more. Another example is, if you run a web or FTP server, select **Group By Local Port**, then click the port name in the left panel ("www", for example) and the information panel shows you how your computer is exactly connected to your server.

If you are looking for applications sending data to a particular computer on the Internet, you can do this almost immediately if you use the **Group By** selection of the **View** menu.

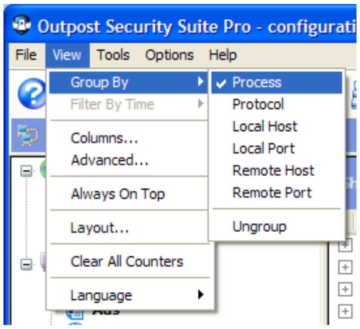
Group By can be used on the following left panel items:

- Network Activity
- Open Ports

Group By changes the type of the following objects display:

- Process
- Protocol
- Local Host (your computer)
- Local Port (on your computer)
- Remote Host (another computer than yours)
- Remote Port (on the other computer)

Highlight one of the left panel items listed above, click the **View** menu and select **Group By**:



You can also get this same display by highlighting the left panel category, **Network Activity** in our picture, and then clicking the **Group By** button on the tool bar.

Appendix B: Types of ICMP Messages

Field Value	Description
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect
8	Echo Request
10	Router Solicitation
11	Time Exceeded For Datagram
12	Parameter Problem On Datagram
13	Timestamp Request
14	Timestamp Reply
16	Information Reply
17	Address Mask Request
18	Address Mask Reply

Echo Request is one of the simplest methods of checking operating conditions of a network node. Once an echo signal is received, any network node generates an **Echo Reply** and returns it to the source. If the source receives a reply to the echo request, this indicates that the main components of the traffic system are in good condition.

Destination Unreachable is generated by a gateway when it cannot deliver an IP datagram. This is the unit of data, or packet, transmitted in a TCP/IP network. Each datagram contains source and destination addresses and data.

A **Source Quench** ICMP message is transmitted from the node to the datagram source in the event that the input queue is overcrowded. In this case, the datagram is removed from the queue.

A **Redirect** ICMP message is transmitted when a gateway detects that a non-optimal route is used, then the gateway sends a request for a change of route in the routing table.

An **IP Announcement** ICMP message transmits a broadcast to announce its IP address.

The **Time Exceeded For Datagram** ICMP message is sent when a datagram is transferred from one gateway to another more times than it is allowed (normally this indicates route cycling).

A **Parameter Problem on Datagram** ICMP message is sent by a gateway if a problem occurs during the transmission of a specific datagram that is not in the range of the above messages. The datagram must be abandoned due to this error.

The **Timestamp Request** and **Timestamp Reply** ICMP messages are used to synchronize the clocks in a network's nodes.

The **Information Request** and **Information Reply** ICMP messages are obsolete. They were used earlier by network nodes to determine their inter-network addresses, but are now considered outdated and should not be used.

The **Address Mask Request** and **Address Mask Reply** ICMP messages are used to find out the mask of a subnet (i.e. what address bits define a network address). A local node sends an **Address Mask Request** to a gateway and receives an **Address Mask Reply** in answer.

Appendix C: Penetration Techniques

Outpost Security Suite allows to control the following actions:

Components injection

Windows operating system by design enables installing system interceptors (hooks) through which foreign code can be injected into other processes. Usually this technique is used to perform common, legitimate actions, for example, switching the keyboard layout or launching a PDF file within the web browser window. However, it can be likewise used by malicious programs to embed malicious code and thus hijack the host application. An example of leak test using such technique to stage a simulated attack is a PC Audit program (http://www.pcinternetpatrol.com/).

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

Control over another application

DDE technology is used to control applications. Most famous browsers are DDE servers and can be used by malicious programs to transfer private information into the network. One example of this technique is Surfer leak test (http://www.firewallleaktester.com/leaktest15.htm). ZABypass is another example of a leak test using this method.

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

Application window control

Windows allows applications to exchange window messages between processes. Malicious processes can get control over other network-enabled applications sending them window messages and imitating user input from keyboard and mouse clicks. The example of using this technique is Breakout leaktest (http://www.firewallleaktester.com/leaktest16.htm).

Here the point is program interactivity through the SendMessage, PostMessage API, and so on. This technique is sometimes used for legitimate inter-process interactivity, but can likewise be used for nefarious purposes by perpetrators.

Outpost Security Suite controls such attempts.

Active Desktop modification

Installing the specific HTML file for Active Desktop, malicious processes can transfer private data on behalf of Windows Explorer. The example of using this technique is Breakout leaktest (http://www.firewallleaktester.com/leaktest16.htm).

Outpost Security Suite controls such attempts to steal data by bamboozling the firewall.

DNS query submission

DNS Client service contains potential vulnerability called DNS tunneling. The main point is that malicious code can transfer and receive any information using correct DNS packets to the correctly configured operating DNS server. The example of using this technique is DNSTester leaktest (http://www.klake.org/~jt/dnshell/).

Outpost Security Suite performs double verification of access to the DNS Client service, providing a more secure system. This enables control access to DNS API even with the DNS Client service on, benefiting users who, out of compatibility concerns, cannot disable this service themselves. This functionality allows assigning permissions to a specific process for using the DNS Client service.

Application launch with URL

Malicious processes can launch the default web browser with a pre-configured web address in a hidden window, making the firewall believe a legitimate action is taking place. Firewalls that explicitly trust an application without looking beyond on who actually launched it in the first place and what additional connection parameters are supplied are unable to challenge the technique, meaning sensitive data could leave the computer past them. The examples of using this technique are Tooleaky and Ghost leak tests (http://www.firewallleak tester.com/leak test2.htm, http://www.firewallleak tester.com/leak test13.htm).

Outpost Security Suite watches every program started on a computer and controls who has the permission to start a program with a target URL and will prompt a user if such activity should be permitted for a particular program.

Application launch with command line parameters

Several firewalls are exposed to a vulnerability of a predatory code launching the default web browser with command-line parameters, allowing to circumvent the existing protection because the firewall is made to believe the legitimate application is performing the legitimate actions. However, in those command-line parameters some piece of private or critical data may be contained, along with the host name as a target recipient of thereof. The example of using such technique is Wallbreaker leaktest (http://www.firewallleaktester.com/leaktest11.htm).

Outpost Security Suite provides the restricted list of processes that are allowed to start default browser with command line parameters protecting your browser against tampering. Beyond traditional browsers, command-line launch control applies to all network-enabled applications which are present in the configuration.

Critical registry entry modification

Malicious processes can modify registry to get network access on behalf of other application, for example, Windows Explorer. The example of using this technique is Jumper leaktest (http://www.firewallleaktester.com/leaktest17.htm).

These attempts are controlled by Outpost Security Suite . This proactive capability offers to select whether you want to allow embedding an object into a certain area of the registry.

OLE application control

A relatively new technique to control applications' activity through the OLE mechanism (a short form of Object Linking and Embedding command) - 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 activity of the Internet Explorer web browser so that it can send user-specified data to the remote location. The example of using this technique is PCFlank leaktest (http://www.pcflank.com/PCFlankLeaktest.exe).

Outpost Security Suite detects an OLE communication and prompts a user whether it is normal for the application to control other application's activity.

Process memory modification

Several Trojan horses and viruses use sophisticated techniques that let them alter the code of trusted applications running in memory and thereby bypass the system security perimeter and perform their malicious activities. This is also known as code injection or copycat vulnerability. The examples of using this technique are Thermite and Copycat leaktests (http://www.firewallleaktester.com/leaktest8.htm, http://www.firewallleaktester.com/leaktest9.htm).

Outpost Security Suite enables you to control the functions that can be used to write malicious code into trusted application address space and so prevent a rogue process from injecting their code into trusted processes. The entire memory space used by any active application on a computer is scrutinized by Outpost Security Suite (not just that of a network-enabled application). In case of malware trying to modify any legitimate application's memory, Outpost Security Suite detects it and display a pop-up prompt asking for your decision. 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 detected by antivirus and anti-spyware vendors.

Low-level network access

Some network drivers allow direct access to network adapter bypassing the standard TCP stack. These drivers can be used by sniffers and other malicious programs to get low-level network access and pose an additional risk for the system as traffic passing through them cannot be screened by a firewall. The example of using this technique is MBtest leak test (http://www.firewallleak tester.com/leak test10.htm).

Outpost Security Suite allows controlling applications requesting network access bypassing standard methods. This feature strengthens the overall network security level preventing outbound data leakage. The user is able to control an application's attempts to open a network-enabled driver, meaning that without the user's authorization, an application is not able to send even the ARP or IPX data.

Appendix D: Technical Support

If you need assistance in using Outpost Security Suite, 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.