



OUTPOSTPRO

NETWORK SECURITY

Administrator Guide

Abstract

This document provides information on deploying Outpost Network Security in a corporate network. It also describes the general process of configuring client software.

Table of Contents

System Requirements	4
Architecture	4
System Requirements	4
Installing Outpost Network Security	5
Deploying Outpost Network Security Client on Client Computers	8
Scanning Client Computers	10
Configuring Protection Settings for Client Computers	15
General Settings	15
Configuration	16
Firewall	17
Network Rules	19
Managing Global Rules	19
Managing Low-Level System Rules	22
Controlling ICMP Protocol Activity	22
Attack Detection	23
Specifying Attack Detection Level	24
Protecting from Ethernet Attacks	25
Port Scanning	26
Attacks List	28
Specifying Trusted Hosts and Ports	29
LAN Settings	30
Detecting a Local Area Network	30
Specifying LAN Access Levels	32
IP Blocklist	33
Host Protection	34
Setting Local Security Level	35
Controlling Penetration Techniques	35
Controlling Critical System Objects	36
USB Device Lock	37
Anti-Malware	38
Schedule and Profiles	39
Mail Scanner	40
Web Control	42
Setting Web Control Level	43
Specifying Exclusions	44
Ads and Sites	45
Site Blacklist	46
Logs	47
Monitoring Client Computers	48
Managing Groups of Computers	50
Configuring Updates for Client Computers	51
Server-Side Logging	52
Appendix	53
Troubleshooting	53
Understanding Penetration Techniques	53
Using Macro Addresses	56
About Agnitum	57

System Requirements

Architecture

Outpost Network Security working environment implies the presence of the following computers:

- computer with Outpost Network Security services running (local update server that provides a centralized (single download, multi-install) client update and local configuration server that is responsible for providing client with configuration settings);
- computer with Management Console installed—the main managing tool that lets you control client installations over your network and manage the other product components;
- one or more clients—computers to be protected.

System Requirements

Physically, Management Console and services can be installed on the same computer. It is not necessary to install Outpost Network Security server part on a domain controller or server; it can be installed on any dedicated workstation running under Microsoft Windows 2000 or later.

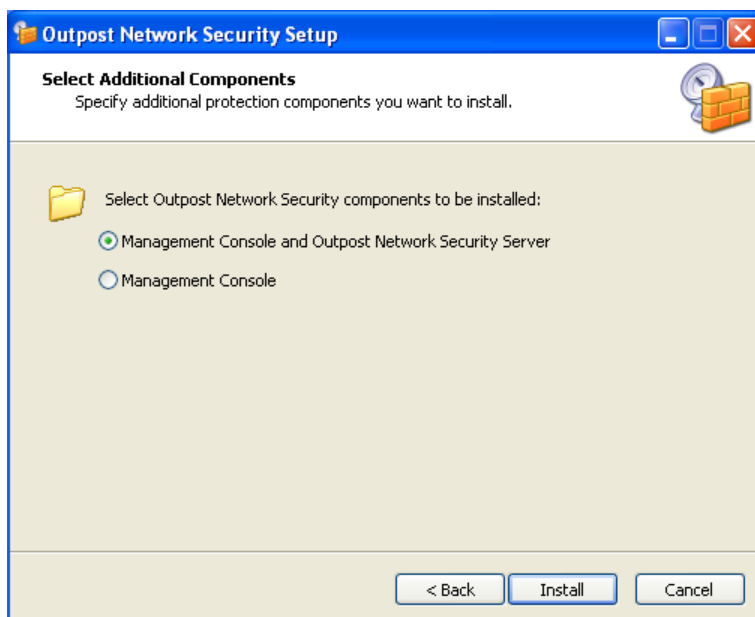
Client part can be installed on a computer with Microsoft Windows 2000 SP4 or later. Also, all 64-bit versions of operating systems are supported.

Installing Outpost Network Security

Before installing Outpost Network Security:

- Make sure that File and Printer Sharing is enabled on the computer (right-click any folder in Windows Explorer, click **Properties** and select the **Sharing** tab);
- Make sure that Windows Firewall is disabled (**Control Panel > Windows Firewall**).

To start installing Outpost Network Security, run the setup file. The installation procedure is straightforward and similar to most Windows installers. Just follow the steps of the setup wizard and it will install all the required components on your computer. You will be prompted to select components to install: you can either install Management Console and services on the same computer or install Management Console on a separate computer.



Important: Both Management Console and services should be installed on a computer with static IP address.

During installation, the Outpost Network Security Client installation package will be copied to the **C:\Program Files\Agnitum\Outpost Network Security\clients** folder, which is automatically shared, so the installer is available to all clients on the network.

After copying files, the setup wizard will prompt you for the port numbers to be used by the client computers to connect to the server and a password to be used to control access to the Management Console.



Outpost Network Security Setup Wizard

Configure Server Settings
Please specify network settings and administrator password.

Service ports
Please specify ports that will be used by clients to connect to Outpost Network Security services.

Configuration service port:

Update service port:

Security
Specify password that will control access to Management Console.

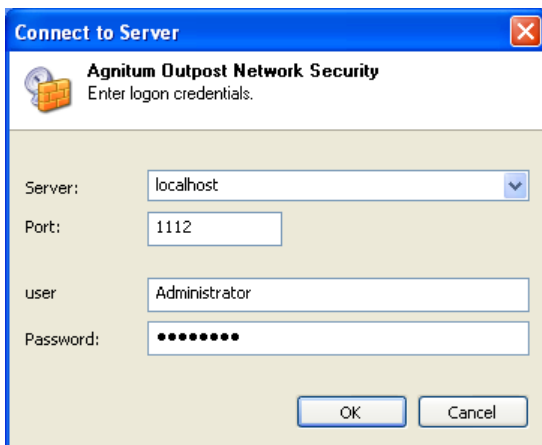
Password:

Confirm password:

< Back Next > Cancel

Note: You can specify additional accounts that will have access to Management Console later. To do this, click **Settings** on the Management Console's toolbar, select the **Security** tab, click **Add**, specify the username and password, and click **OK**.

On completing the setup wizard, you will be prompted for server part connection parameters and will be able to specify access credentials to start Management Console.



Connect to Server

Agnitum Outpost Network Security
Enter logon credentials.

Server:

Port:

user:

Password:

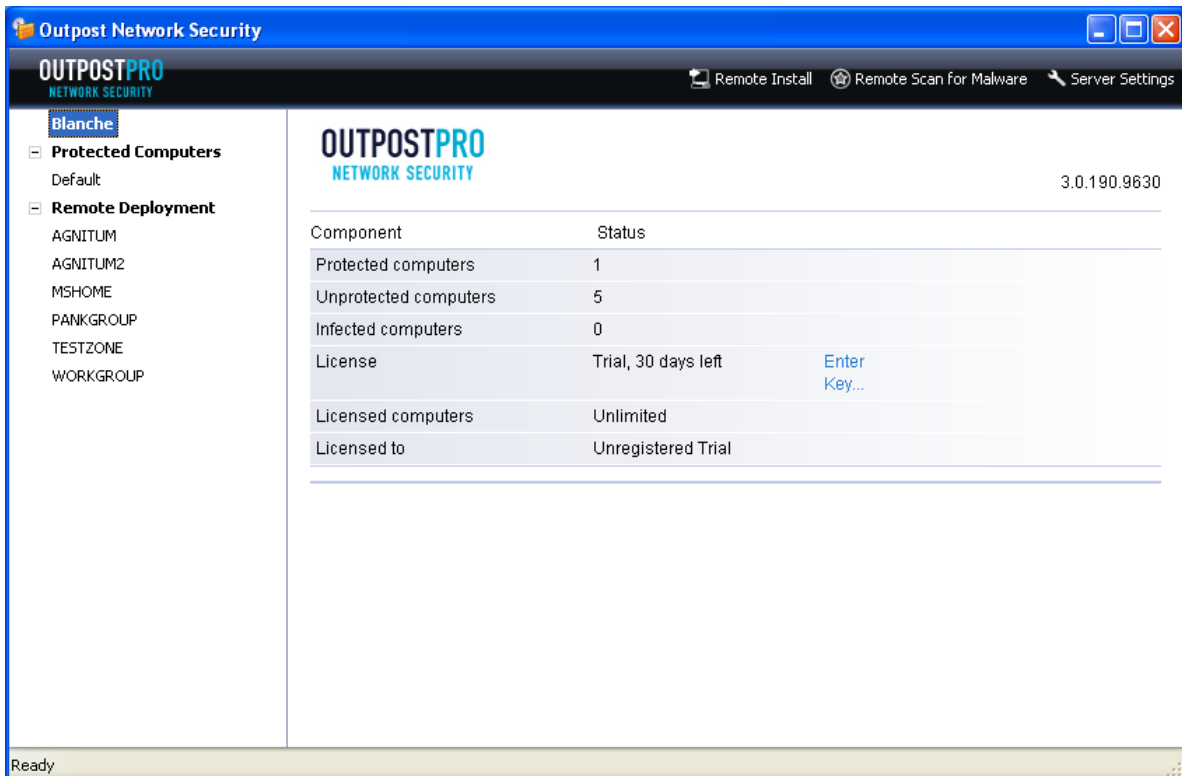
OK Cancel

Type in IP address, DNS name or NetBIOS name of the computer with Outpost Network Security services installed or select it from the drop-down list. If server part is installed on a local computer, select **localhost**.

Also, specify the port to be used by configuration service and credentials (password, specified during server part installation).

Note: Outpost Network Security itself does not install Outpost Network Security Client on the console. Client software can be installed on the same computer where Management Console or Outpost Network Security services are installed either manually or using the procedure described in [Deploying Outpost Network Security Client on Client Computers](#) section. However, if any security software is installed on the console, make sure that the connection to the port specified as a configuration service port is not blocked. Otherwise, clients will not be able to get the configuration settings and function properly.

Once you enter the credentials and click **OK**, the Management Console main window will be displayed.



OUTPOSTPRO NETWORK SECURITY 3.0.190.9630

Component	Status
Protected computers	1
Unprotected computers	5
Infected computers	0
License	Trial, 30 days left Enter Key...
Licensed computers	Unlimited
Licensed to	Unregistered Trial

Ready

In the right panel of the main window you can see some general statistics on your network and license information. If you want to enter the license key, click **Enter Key**.

Note: If no valid license key is specified, the client software will not get new updates and configuration settings.

Deploying Outpost Network Security Client on Client Computers

Before deploying Outpost Network Security client software to computers on your network, check the following on each client:

- Make sure that account with administrator privileges is created and the password is set;
- In **Control Panel > Administrative Tools > Local Security Policy > Security Options** change the **Network access: Sharing and security model for local accounts** local policy from **Guest only – local users authenticate as guest** to **Classic – local users authenticate as themselves**;
- Make sure that Windows Firewall is disabled (**Control Panel > Windows Firewall**).

For a small number of computers, you can install Outpost Network Security client on each user's workstation manually (the client setup package file,

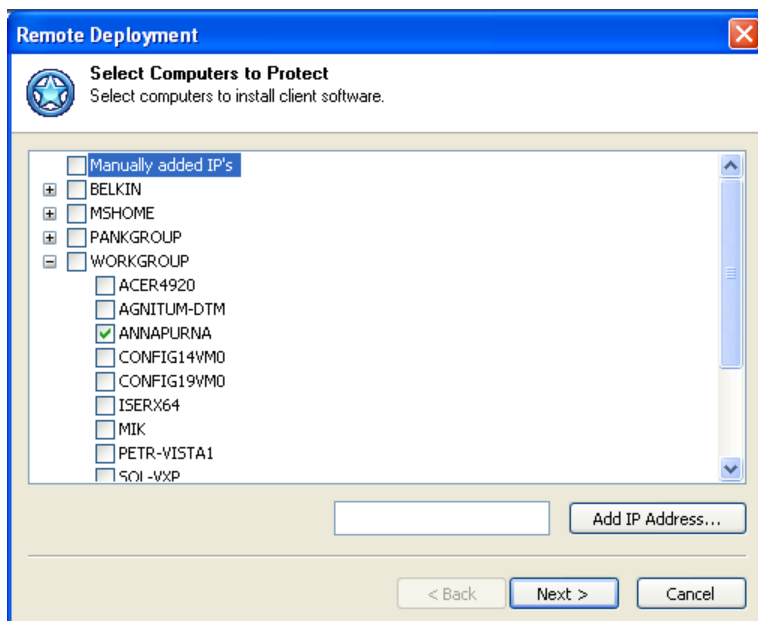
OutpostNetworkSecurityClientInstall.exe, is located in the **C:\Program Files\Agnitum\Outpost Network Security\clients** folder, which is shared during installation).

Outpost Network Security allows for automatic installation of the client part on the workstations. All workstations on your network are enumerated and listed under the **Remote Deployment** node in the left panel of the Management Console's main window. Also, they are grouped into domains and workgroups represented as sub nodes of this node according to your network infrastructure.

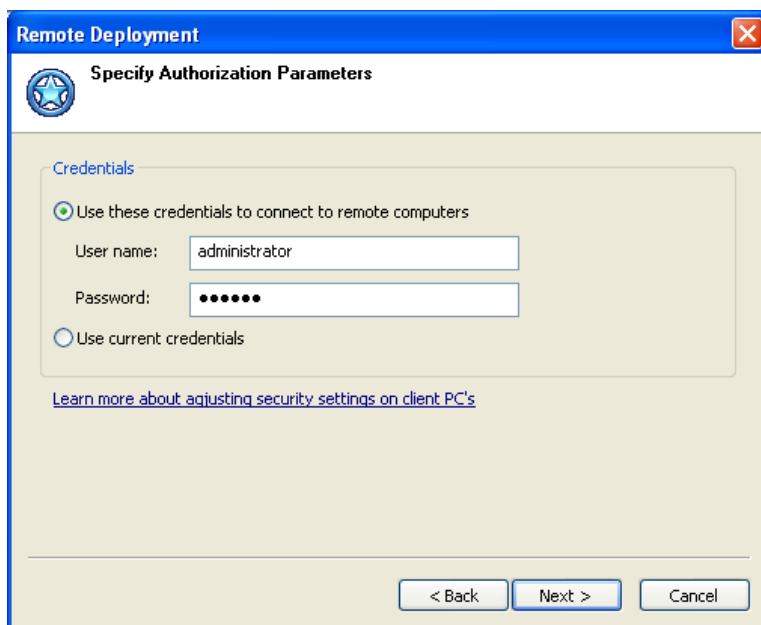
Use the **Refresh Network Environment** command available on the node's shortcut menu to refresh the information.

To automatically install the client part on the workstations, click **Remote Install** on the Management Console's toolbar or select **Install Outpost Network Security** on the node's or particular computer's shortcut menu and follow the **Remote Deployment Wizard**.

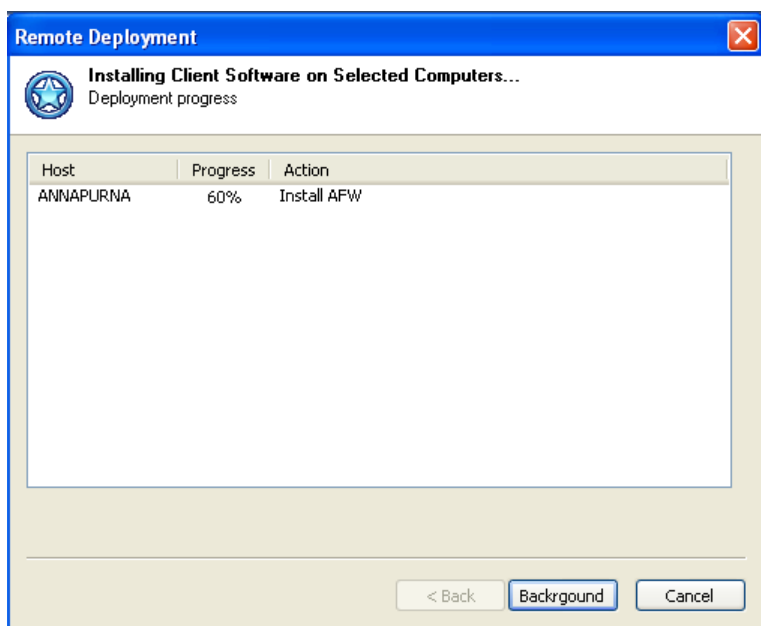
The first step allows to select computers on your network to install client software. You can also specify the IP address manually in the provided text box below if you don't see the computer in the tree. After clicking **Add IP Address**, the IP will appear under the **Manually added IP's** node.



After clicking **Next**, you will be prompted for the credentials to connect to all the selected computers. The specified account should possess administrative rights on all the computers.



Click **Next** to start remote installation.



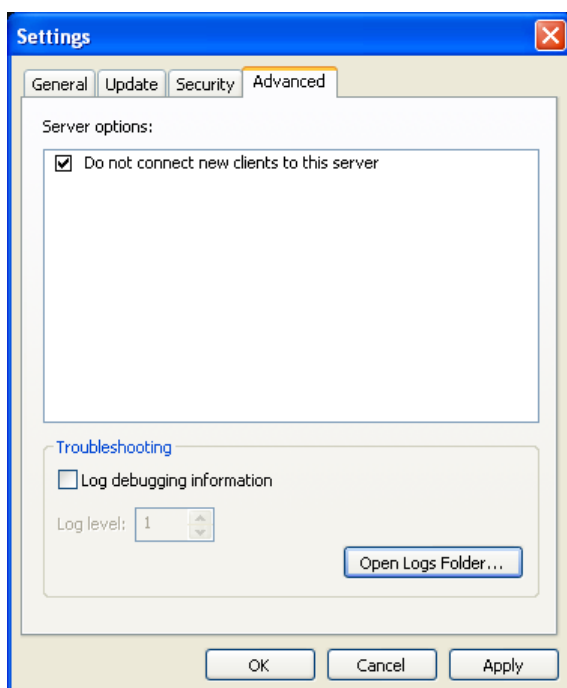
After client installation, all the computers where it was installed successfully will be listed under the **Default** group of the **Protected Computers** node. After selecting this group in the left panel, you will see the list of computers belonging to it.

The **Protected Computers** node display basic statistics for all the clients and a list of recent protection events occurred on the client computers.

Notes:

- Make sure to manually uninstall all previous Outpost versions from those computers you are going to protect. In this case the configurations for those computers are not automatically supported. Also be sure to uninstall any other security software and reboot before installing Outpost Network Security client to prevent a system conflict of different security solutions fighting to control network access.
- If you do not want “unknown” clients that were not deployed by this particular console to be connected to it, click **Settings** on the Management Console’s toolbar, select the

Advanced tab, and select the **Do not connect unknown clients to this server** check box.

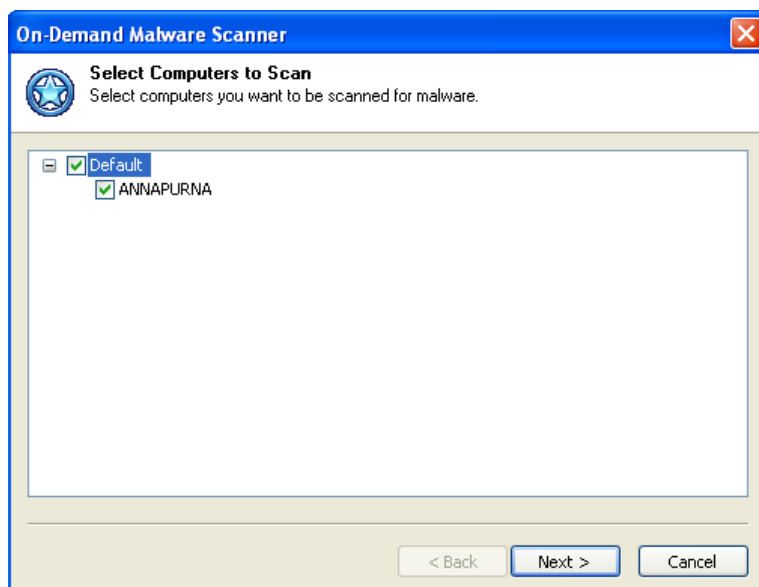


Scanning Client Computers

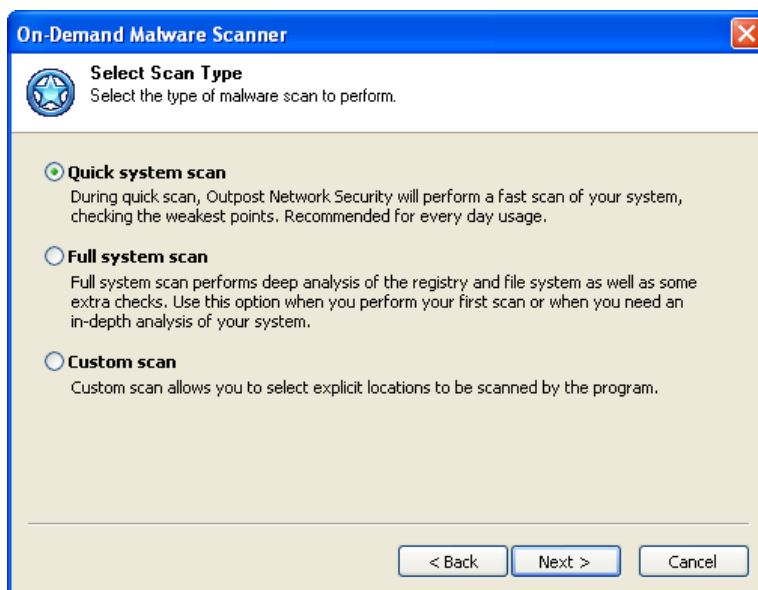
On-demand global system scanning lets you scan for and remove threats on hard disks, network folders, DVDs, and external storage devices at your own convenience. By excluding locations and file types from the scan (provided you are certain these locations and/or file types are not vulnerable to infection), you can flexibly specify scan areas to meet your specific requirements.

It is recommended to run a full scan just after Outpost Network Security's installation to check the systems for whatever malware they already have. To do this, start **On-Demand Malware Scanner** by clicking the **Remote Scan for Malware** button on the toolbar. The wizard will help you specify the scan settings and guide you through the whole process of the system scan.

The first step allows to select computers or groups of computers to be scanned.



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



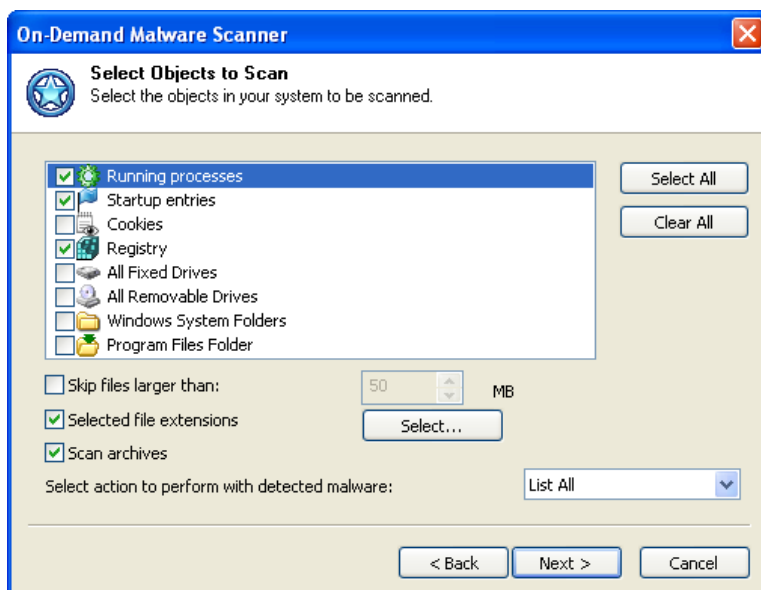
- **Quick system scan.** This option performs a fast scan of the system by checking only the most vulnerable points such as running processes in memory, susceptible registry keys, and target files and folders. This option is recommended for every day usage.
- **Full system scan.** A full system scan is a deep analysis of the registry and file system as well as some extra checks (processes in memory check, cookies scan, startup entries scan). This check should be performed when you scan the system the first time. The operation can take considerable time depending on the speed of processor, the number of applications installed on the computer and the amount of data stored on drives.
- **Custom scan.** This option enables you to explicitly select the locations to be scanned. You can select either of the options above or you can choose specifically what to scan on the remote systems.

Tip:

- To improve scan performance, you can have Outpost Network Security create scan status cache files in each scanned folder by selecting the **Enable SmartScan technology** check box on the **General** tab of the product settings. Note, that the cache files are invisible and therefore may cause false positives from anti-rootkit tools.

After selecting the scan type, click **Next** to proceed.

If **Custom scan** is selected, the **Select Objects to Scan** step appears for you to explicitly select the objects, disks, and folders you want to have scanned and the actions to be performed on any detected malware objects. The same settings are available for editing a scan profile in the **Edit Scan Profile** window:



If you do not want to scan files larger than a specific size, select the **Skip files larger than** check box and specify the minimum file size to be skipped. You can also limit scans to specified types of files by selecting the **Select file extensions** check box. To edit the list of file extensions to process, click the **Extensions** button. The most common types of files that can contain malicious code are already added to the list for your convenience, but you can add, edit, or remove file extensions according to your needs. To revert to the original list, click the **Default** button.

To configure scanner behavior, specify the action to perform on found malware. The following actions can be performed on suspicious programs:

- **List All.** In this case, all the detected objects will be listed after the scan is finished and you will be able to process each object individually.
- **Cure.** On detecting a suspicious program, Outpost Network Security will try to cure the suspicious object. If the object cannot be cured, Outpost Network Security will automatically quarantine it.
- **Remove.** Detected objects will be deleted from the disk.
- **Quarantine.** Outpost Network Security will place the detected malware in quarantine.

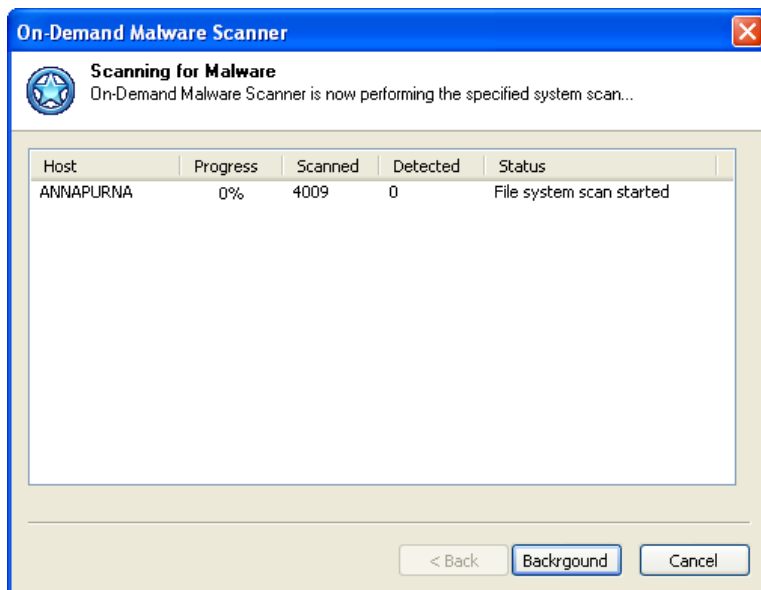
If you think your archive files may contain malicious programs, you can also select the **Scan archives** check box.

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

Note:

- Spyware (a specific type of malware) cannot be cured and is automatically quarantined.
- The specified action does not affect critical objects and cookies. If a critical object or cookie is detected during scanning, no action will be taken and the **Specify Actions for Detected Objects** step will be displayed after the scan is finished as if the **List All** action were selected.
- Irrespective of the specified action, all malware activity is blocked immediately after it is detected.
- Outpost Network Security scans files contained in ZIP, RAR, and CAB archives.

After clicking **Next**, Outpost Network Security starts to scan the selected objects and locations. The progress step displays the following stats for each scanned computer as the scan continues: the total number of objects scanned and the number of detected potentially malicious objects:

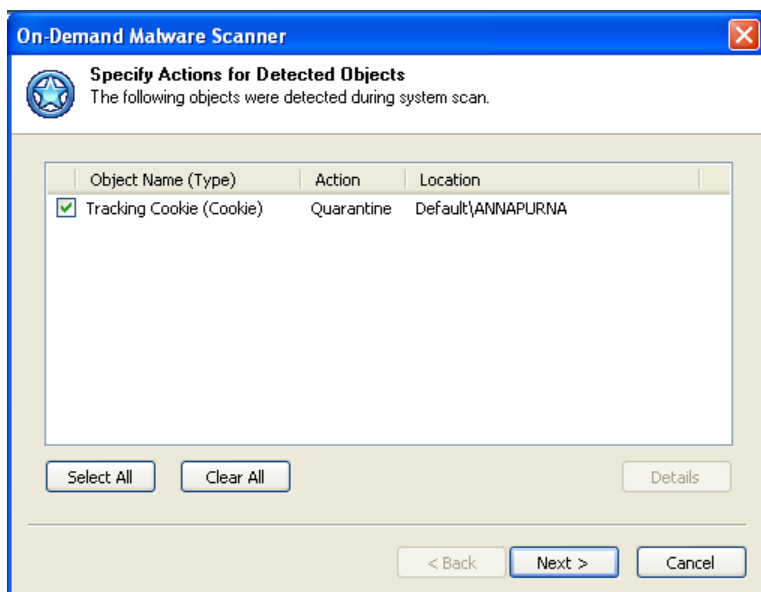


The scanning process can run in background mode. If you want to work with Outpost Network Security while the scan is underway, click the **Background** button and the wizard will be minimized. To see the full window again, click the **Remote Scan for Malware** button on the toolbar again.

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

When the scan is complete, a list of detected objects (if any are found) is displayed automatically. If all systems are clean (i.e. no suspicious objects were found), only 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 user systems. Next to each malware is displayed the category it belongs to, and the action to be performed on it:



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

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

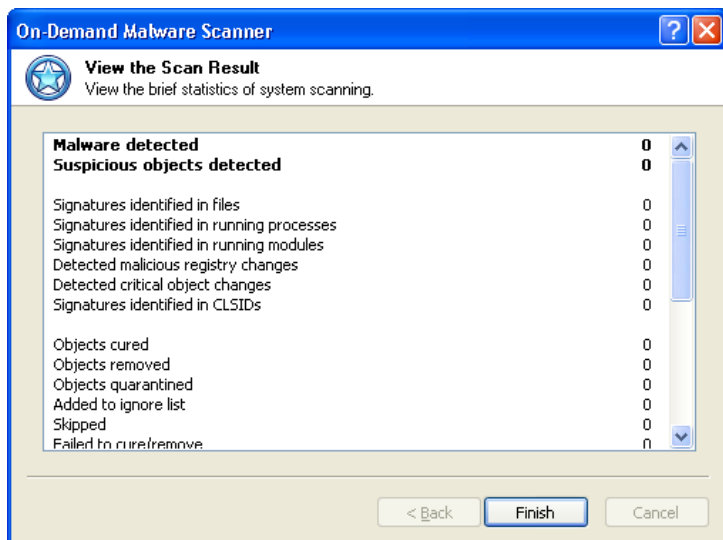
Select the check boxes next to the objects you want to process and click **Next**. Outpost Network Security then performs the specified actions—cures the object, removes it from the places it is registered in and from memory or places in quarantine so you can restore it later if you find some software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

Any software that you did not select will be left intact and will continue to be active on the system.

Important:

- A cookie is not spyware, but it can be used as a holding file to transfer private information from your computer to a specific web site. Spyware programs installed on your computer can write your private information into cookie files, which can later be read by the site that owns those cookies the next time your browser visits that site (whether you knowingly go to the site or your browser is simply directed there).

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

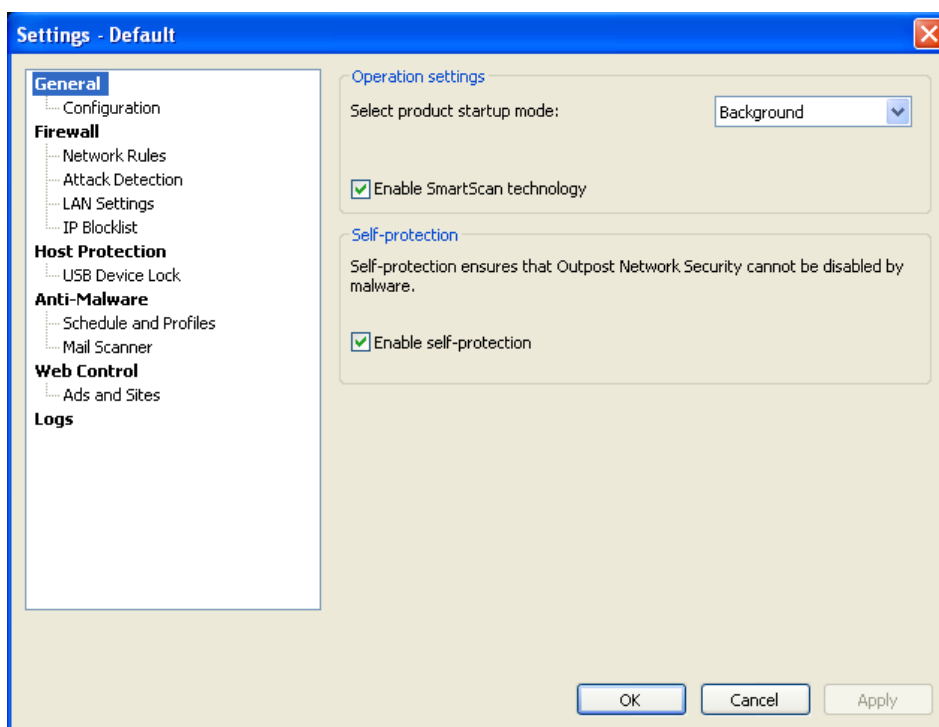


Configuring Protection Settings for Client Computers

Information about client computers currently connected to the console is available if you select the **Protected Computers** node of the Management Console tree. All client computers are organized into groups under this node. After being installed, all clients are automatically placed into the **Default** group.

Note: For details on combining client computers in groups, see [Managing Groups of Computers](#).

Security settings on client computers are configured using the **Settings** command on the group's shortcut menu. In the opened window you can see all the Outpost Network Security Client settings, so the configuration process of the computers belonging to the selected group is convenient and easy to use for those administrators who are already familiar with earlier Outpost software versions.



After the settings are specified, click **OK** and the newly created configuration will be available for all computers in the group and will be applied without restart.

If you create a new group and want to assign settings of an existing group to all its computers, right-click the existing group name, select **Copy Settings**, and click the name of the new group to assign settings.

To restore the default settings for the selected group, right-click its name and select the **Set Default Settings** command.

All the settings that are available for remote configuration are discussed below.

General Settings

By default, Outpost Network Security Client is automatically loaded when the client computer starts up and operates silently, in **Background** mode, providing immediate protection at the earliest stage possible. No product icon is displayed in the system tray in this case.

Outpost Network Security allows you to control clients' behavior when the system starts up. You can also select the **Normal** mode to display Outpost Network Security Client icon in the system tray when user turns on the computer.

To improve malware scan performance, you can have Outpost Network Security create check status cache files in each folder by selecting the **Enable SmartScan technology** check box. Note, that the cache files are invisible and therefore may cause false positives from anti-rootkit tools.

To withstand the threat of being switched off, Outpost Network Security features self-protection. With self-protection turned on, Outpost Network Security Client 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 Network Security also constantly monitors its own components on the hard drive, the registry entries, memory status, running services, and so on, and disallows any changes to these by malicious applications.

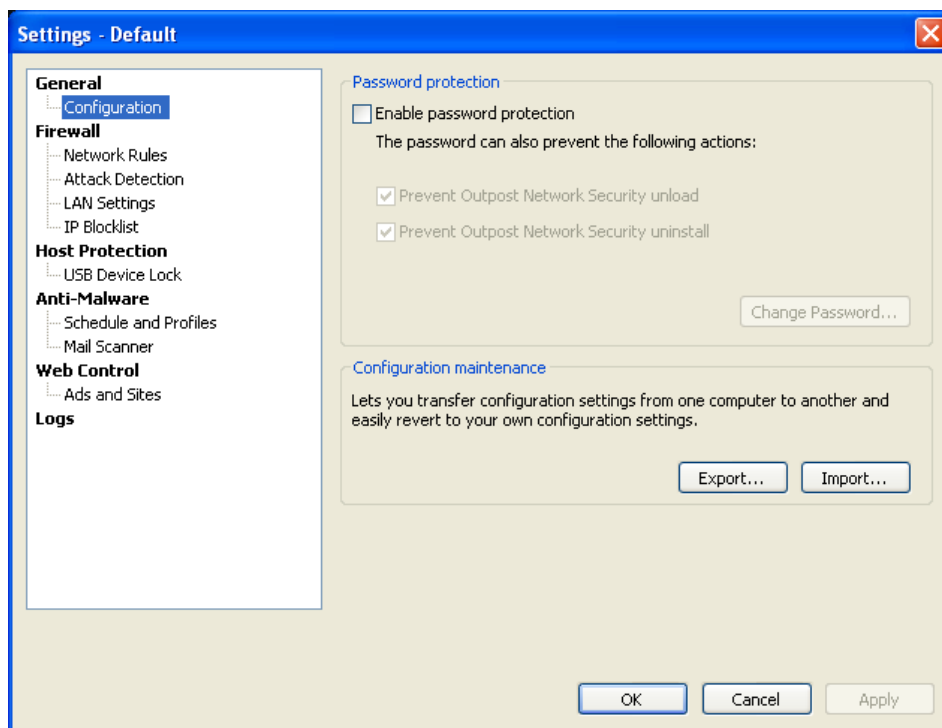
By default, self-protection is enabled and access to components is forbidden for all applications. To disable self-protection, clear the **Enable self-protection** check box.

Note:

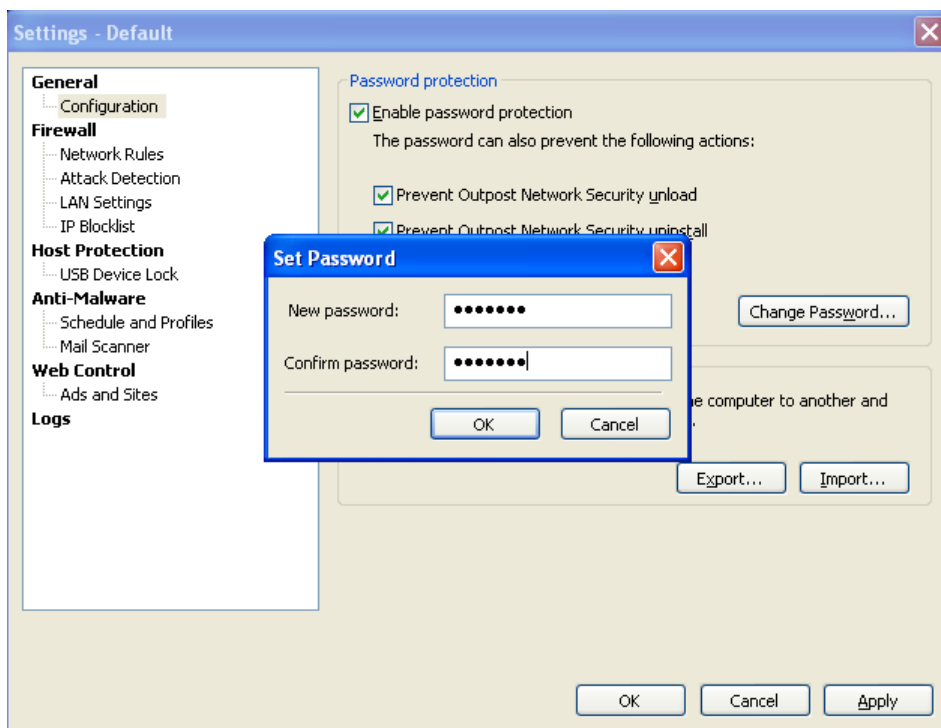
- Disabling self-protection may severely impact your overall system security. Though disabling is required for the installation of plug-ins and other advanced functions, it should be re-enabled as soon as the changes have been made.

Configuration

Outpost Network Security enables you to protect the settings you specify from being altered without your permission. Being secured by a password, product settings cannot be changed by users of the client computers.



To set the password, select the **Enable password protection** check box. Specify the password in its dialog box, confirm it and click **OK** to save it. After that, every time somebody tries to gain access to the product settings, he will be prompted for this password.



To change the password, click **Change password** under **Password protection**. Specify and confirm the new password, then click **OK**.

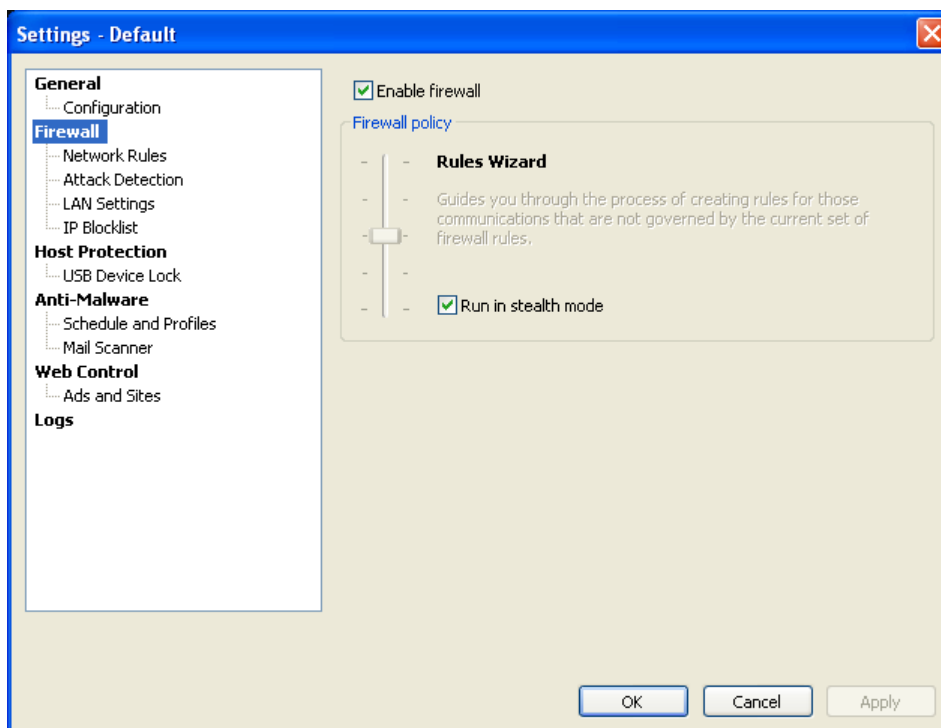
To disable the password, clear the **Enable password protection** check box.

You can additionally protect Outpost Network Security Client from being unloaded and uninstalled by selecting the corresponding check boxes. This prevents unauthorized persons from disabling the protection and the restrictions you set and is most useful for employers who need to restrict the activities of their employees.

You can create several configurations by changing specific settings and giving each configuration a different name using the **Export** command. To switch to another configuration, click **Import** and browse to the configuration file.

Firewall

To enable the firewall on the client computers, select the **Enable firewall** check box.



To eliminate the connection request prompts during the Outpost Network Security Client operation, it runs in Auto-Learn mode memorizing (auto-learning) typical activities performed by a system.

In this mode, Outpost Network Security Client assumes all new program activity is legitimate and consequently allows network access and process interaction to all requesting programs. As different programs access the internet and interact with other software for the first time, Outpost Network Security Client memorizes their identities and creates allowing rules for all the requested connections. If the rule exists for the requested connection, the connection is managed according to these created rules, so users' programs will continue to be able to access the internet without triggering a "new connection" prompt.

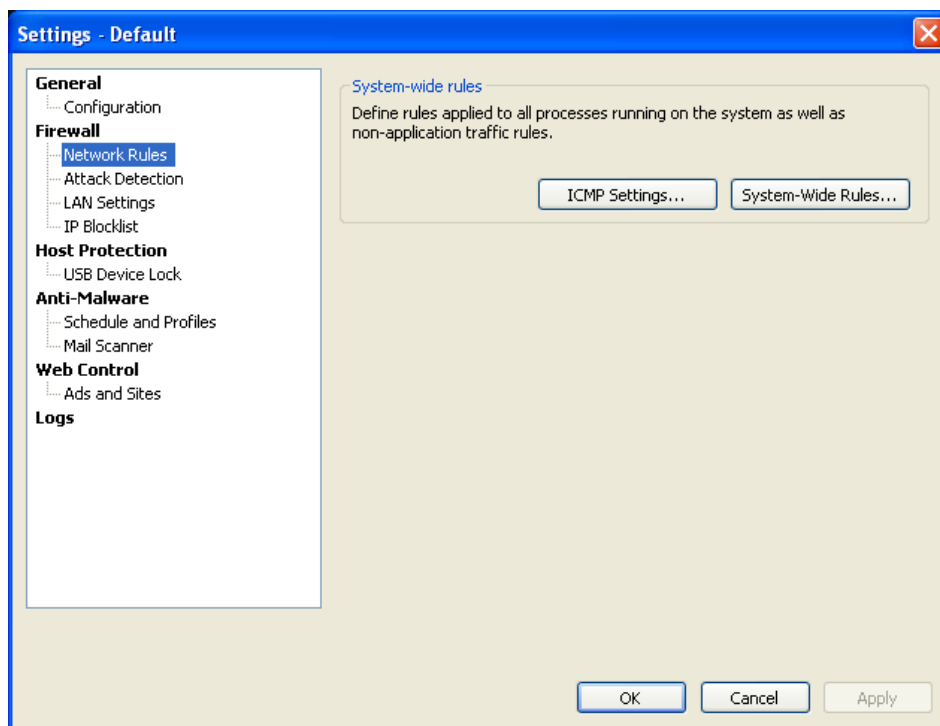
By default, Outpost Network Security Client is operating "stealthily", which means that your computer does not respond to port scans and silently blocks them, making itself invisible to hackers. Normally, when computer receives a connection request to a port that is not used for any incoming or outgoing connections, it lets the other computer know that the port is not used by sending a "port unreachable" notification. In stealth mode, the computer will not respond, making it seem like it is not turned on or not connected to the internet. In this case, packets sent to the unused port are simply ignored by the firewall without notifying the source via an ICMP or TCP message.

To switch the stealth mode, select/clear the **Run in stealth mode** check box.

Note:

- It is recommended that you keep clients in stealth mode unless you have some reason not to.

Network Rules



Note:

- Application rules are computer-specific and can be configured for a particular computer only. For details, see [Monitoring Client Computers](#).

Outpost Network Security Client's firewall enables you to control all user systems' traffic, including:

- Define rules for all processes running on your system ([global rules](#)).
- Define non-application traffic rules ([low-level system rules](#)).
- Control your system's [ICMP traffic](#).

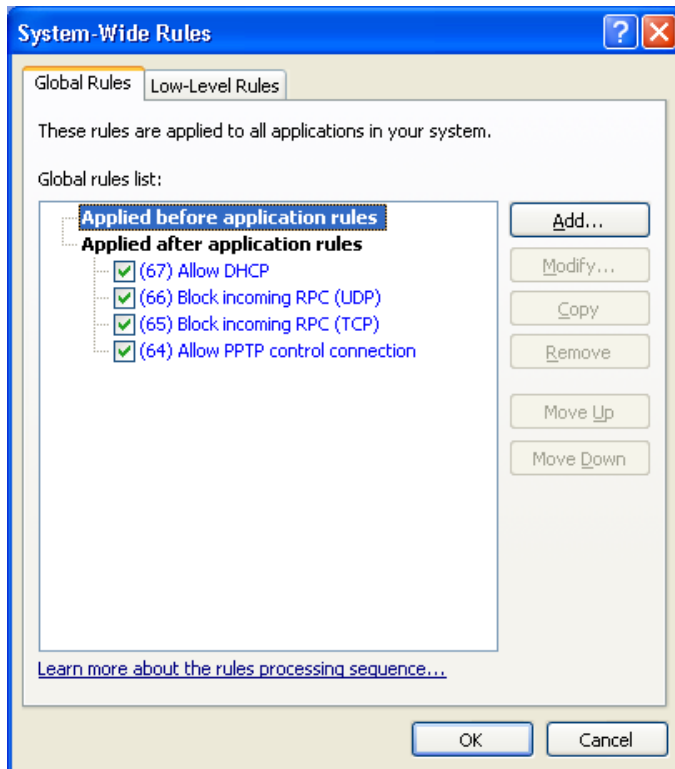
See each corresponding section for details.

Note:

- These settings are for advanced users only. If a setting is changed incorrectly, it could result in your firewall not protecting your system as expected. In most cases, you do not need to modify these rules or add yours.

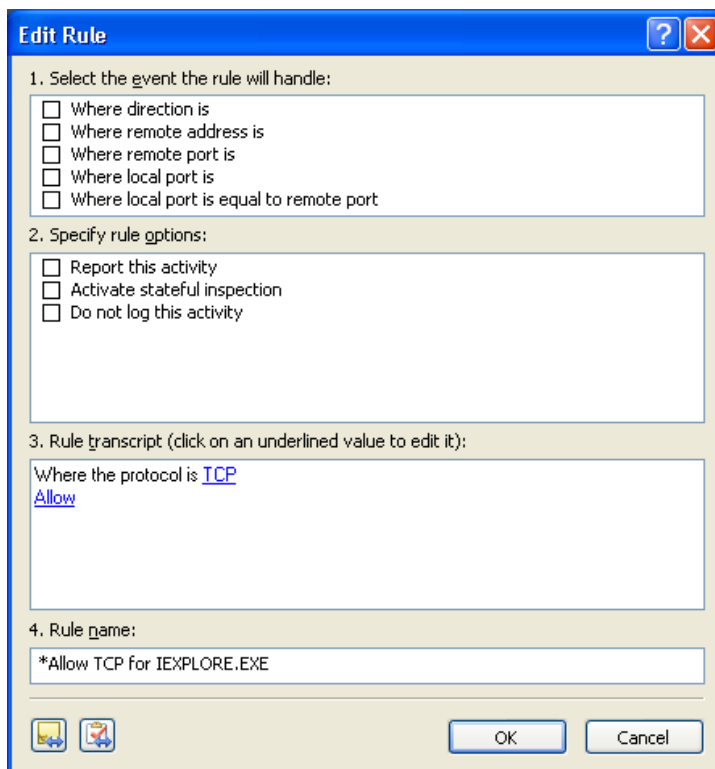
Managing Global Rules

Global firewall rules are applied to all processes and applications on user computer that request network access. You can, for example, block all traffic that uses the TCP or UDP protocol or all traffic from a particular remote host by creating the appropriate rules. Outpost Network Security provides several predefined global rules designed for optimal system functioning. To view the global rules list, click **System-Wide Rules**:



Adding a new rule

To create a new rule, click **Add**:



In the rule editor, specify the following rule parameters:

Event the rule will handle

The following criteria are available:

- **Where direction is** – either outbound (data being sent) or inbound (data being removed).
- **Where remote address is** – a specific IP address or DNS name.
- **Where remote port is** – the port on the other computer that will be used.
- **Where local port is** – the port on your computer that will be used.
- **Where local port is equal to remote port** – both computers use the same port number. If port ranges are specified for the remote and local computers, the rule will be triggered for ports that intersect the two ranges. If the intersection is empty, the rule will not be triggered.

Select the criteria of the event and define all the settings in the **Rule description** text box by clicking the underlined links.

Note:

- For information on using macro addresses to specify local or remote host, see [Using Macro Addresses](#).

Rule options

The following actions are available:

- **Report this activity** – the product displays a visual alert when a rule is triggered.
- **Activate stateful inspection** – turns on "stateful inspection" for this application (after an application connects to a remote server, all incoming data from that server – to the port opened by the application – will be allowed or blocked according to the specified setting).
- **Do not log this activity** – disables activity logging for this rule. If selected, no data will be written to the log when this rule is triggered.

Rule description

When you select the event in the above text boxes, corresponding messages will be displayed in the **Rule description** text box. Below the specified commands you will need to state whether to allow or block the connection by clicking one of the underlined links (**Allow** is the default).

Make sure there are no undefined parameters in the **Rule description** text box. Outpost Network Security will generate a descriptive **Rule name** automatically based on the specified parameters.

Click **OK** to save the rule. The rule will be displayed on the list. The selected rule transcript is shown at the bottom of the window.

Modifying an existing rule

To modify an existing rule, highlight it in the list and click **Modify**. Perform any changes in the rule editor described in the rule creation section above and click **OK** to save the changes.

Selected rules are activated (turned on) and processed by the firewall. Clear the check box next to the rule name to turn it off if you do not want Outpost Network Security to process the rule but you don't want to delete it either. You can turn the rule on at any time by selecting its check box.

Rules are applied in top-down order (highest on the list is applied first), **so be aware but note that Outpost Network Security uses the first rule having criteria that match the application's type**

of communication activity and ignores all subsequent rules. To change a rule's priority, highlight the rule on the list and use the **Move Up/Down** buttons.

You can also copy or remove the highlighted rule within an application using the **Copy** or **Remove** buttons. To copy a rule from one application to another, use the copy and paste buttons in the **Edit Rule** window.

Tips:

- Use the rule transcript at the bottom of the dialog to quickly change one of its parameters.
- Rules automatically created by Outpost Network Security are marked **blue** in the list. Rules created by the user are marked **black**.
- It is prudent to save the present configuration before making changes to it.
- For additional information about the rules processing order, see this article: <http://www.agnitum.com/support/kb/article.php?id=1000120&lang=en>.

Managing Low-Level System Rules

Outpost Network Security also allows you to control system traffic transferred by protocol drivers that use IP protocols other than TCP or UDP, transit packets, and other non-application traffic that cannot be controlled at the application level.

To view the low-level rules list, select the **Low-Level Rules** tab.

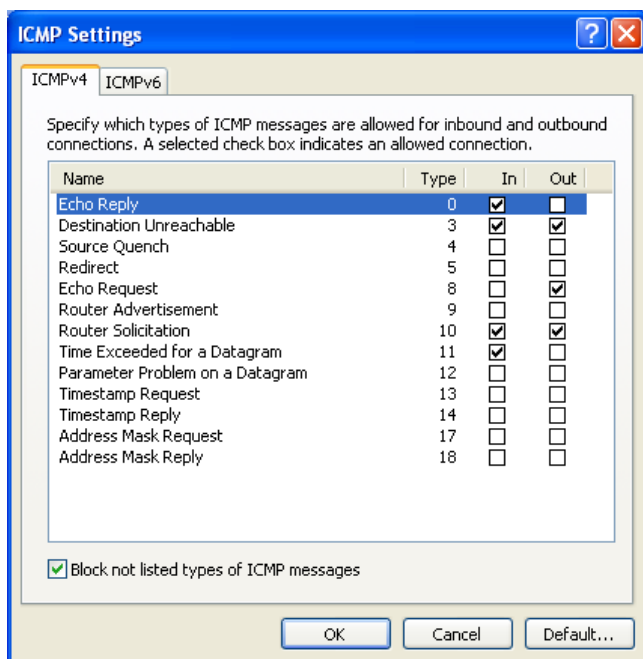
You can add, modify and remove low-level rules the same way as with global rules. The only differences are:

- Rule criteria contain IP protocol type, direction, remote and local addresses.
- **Mark rule as High Priority** sets a rule higher than application and global rules, which take precedence by default.

Controlling ICMP Protocol Activity

Internet Control Message Protocol (ICMP) is used to send error/control messages between computers connected on a network. Outpost Network Security lets you specify the types and directions of the ICMP messages allowed on the client computers.

To specify the ICMP settings, click **ICMP Settings**. In the **ICMP Settings** dialog, the main ICMP message types are listed for both ICMPv4 and ICMPv6 protocols. You can allow incoming or outgoing messages by selecting the corresponding check boxes by their side. If a check box is cleared, the connection is blocked:



Also, you have the ability to restrict ICMPv4 or ICMPv6 protocol communication to the listed types of messages and block all other connections by selecting the **Block not listed types of ICMP messages** check box on the corresponding tab.

Note:

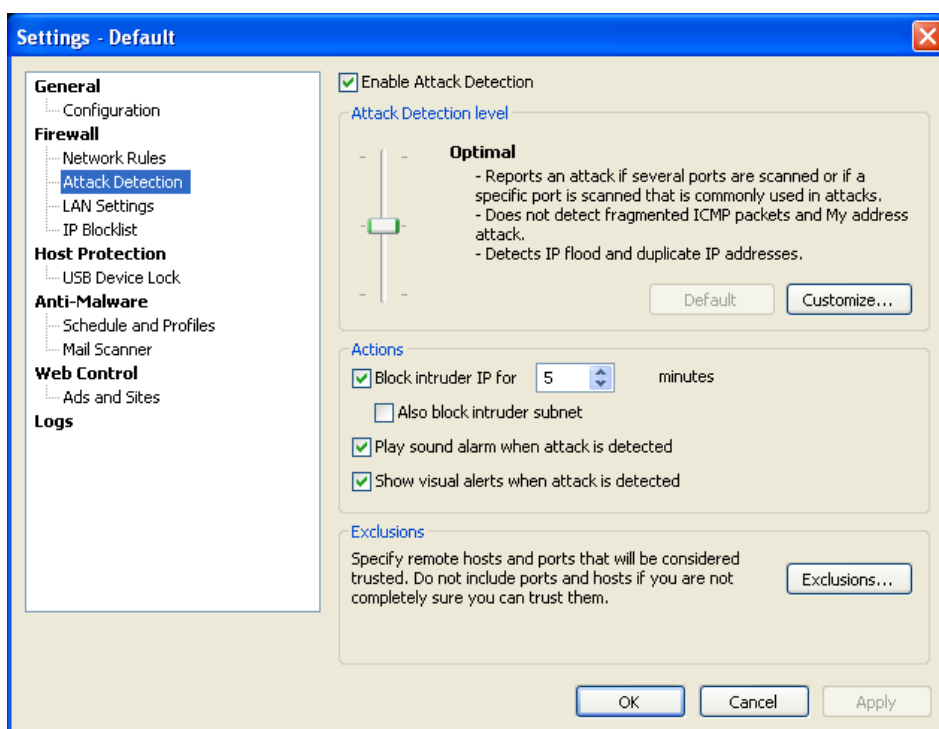
- It is recommended that you do not change the ICMP settings unless you are certain about the changes you are making.

Attack Detection

A major function of firewall protection is inbound filtering, which controls all incoming activity to block hackers and malicious programs when they try to attack user computer.

The Attack Detection component detects, prevents, and reports all possible attacks on user computer from the internet or the network the computer is connected to. It screens inbound traffic and determines its legitimacy either by comparing it against a set of known attack patterns or by performing a behavior evaluation analysis. The Attack Detection component can detect not only every known type of attack (such as port scanning, Denial of Service (DoS), attacks of 'short fragments' and 'my address' classes, and many others), but future exploits as well.

To enable the Attack Detection component, click **Attack Detection** and select the **Enable Attack Detection** check box:



Specifying Attack Detection Level

You can define how sensitive Outpost Network Security should be in detecting attacks by setting the desired attack detection level. The attack detection level determines the types of attacks to be detected and the number of suspicious packets received before Outpost Network Security reports a port scanning attack. To set the attack detection level, move the slider to one of the following values:

- **Maximum.** A port scan alert is displayed even when a single scan of one of computer ports is detected. All Ethernet and external attacks are monitored for and prevented.
- **Optimal.** A port scan alert is displayed only when several ports are scanned or if a specific port is scanned that Outpost Network Security recognizes as one commonly used in attacks. All external attacks are monitored for except fragmented ICMP and My address attacks. IP spoofing and duplicate IP's are watched for.
- **Low.** A port scan alert is displayed only when a multiple scanning is definitely detected. Fragmented ICMP, My address and all Ethernet attacks are not monitored.

Change the attack detection level depending on the risk the computer is under, or if you are suspicious, set the level to maximum.

You may also customize the security level to better meet your requirements by clicking the **Customize** button. The **Ethernet** tab lets you specify settings for [Ethernet attacks](#), the **Advanced** tab will help you define a [list of attacks](#) detected by the firewall and especially protected [vulnerable ports](#).

After Outpost Network Security detects an attack, it can change its behavior to automatically protect user from any future attacks from the same address. To do this, select the **Block intruder for ... minutes** check box and all traffic from the computer attacking user's will be blocked for the number of minutes you designate. The default value is 5 minutes.

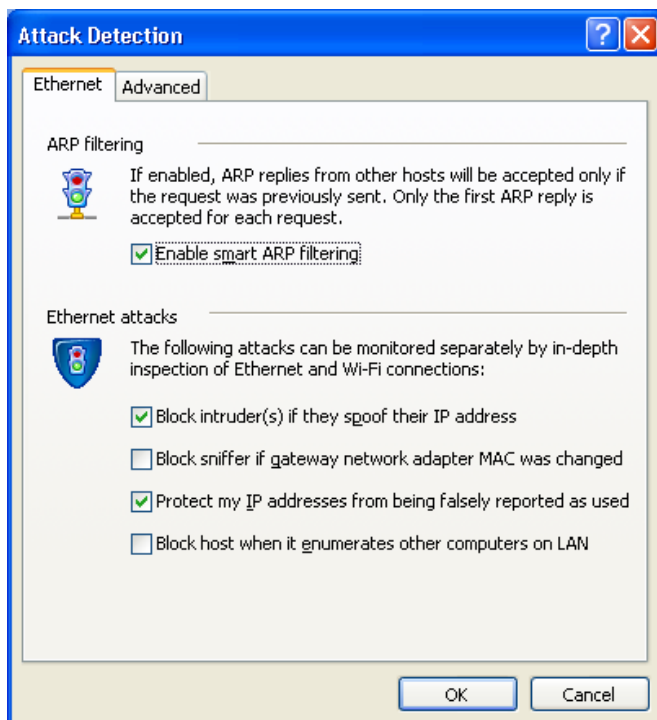
You can also set to block the entire subnet the attacker's address belongs to by selecting **Also block intruder subnet**.

For the user to receive visual and/or sound alerts about detected attacks, select the **Show visual alert when attack is detected** and/or the **Play sound alarm when attack is detected** check boxes under **Actions**.

Protecting from 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.

The Attack Detection component also protects the system from invasions on a local network. It detects and blocks Ethernet attacks such as IP spoofing, ARP scanning, ARP flood and others by inspecting computer's Ethernet and/or Wi-Fi connections. To specify the Ethernet attack prevention settings, click **Customize:**



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 Network Security 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.

- **Block intruder(s) if they spoof their IP address**

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.

- **Block sniffer if the gateway network adapter MAC was changed**

Outpost Network Security 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 Network Security 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 falsely reported as used**

Outpost Network Security 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 Network Security blocks ARP replies that have the same IP (but different MAC's) and thus protects the computer from IP address duplication consequences.

- **Block hosts enumerating other computers on LAN**

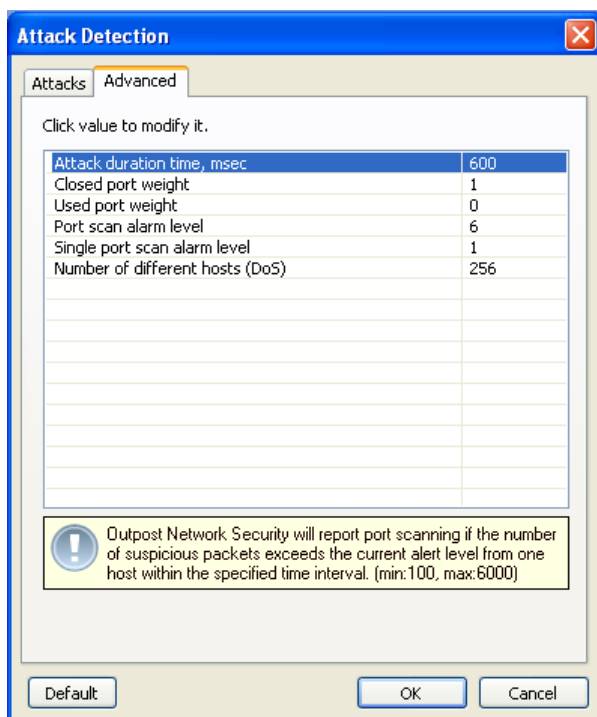
Limits the number of ARP requests enumerating IP addresses from one MAC address during a specified time interval, which can imply network scanning. Some massively propagating viruses use mass host enumeration to hop from one computer to another, infecting them as they go. This technique is also used by scanners and vulnerability analyzers.

Port Scanning

Outpost Network Security's Attack Detection component performs two independent functions: it blocks attacks and detects port scanning. In this context, an attack is the sending of harmful data to user's computer, which can result in system errors (BSOD, system freeze, etc.) or an attempt by an attacker to gain unauthorized access to the data on the computer. Port scanning is an attempt to discover open ports in the system prior to an attack.

On receiving a connection request (a brief message in computer lingo that seeks to establish a connection through one of the ports on the computer), the Attack Detection component logs "Connection request", but to avoid false positives, does not consider this one request a port scan. If multiple connection requests are received from the same remote host, the plug-in will alert user with "Port scanning".

Outpost Network Security's sensitivity in detecting port scanning (which is actually the number of connection requests that trigger a "Port scanning" alert) is defined by the **Port scan alarm level** setting (**Customize > Advanced > Edit List > Advanced**):



By default, the number of port requests from the same host that triggers an alert for each attack [detection level](#) is: 2 for **Maximum**, 6 for **Optimal**, and 12 for **Low**.

Paying special attention to vulnerable ports

From the security point of view TCP and UDP ports in the system are divided into several groups according to the probability of an attacker using the port to break into your system. Typically, ports assigned to vulnerable services like DCOM or RPC should be monitored with greater care because they are more likely to be an attack target.

However, you may have custom services assigned to custom ports that are also a lure for an attacker. The Attack Detection component lets you set selective preferences for different ports and create a list of ports to which Outpost Network Security will pay more attention while monitoring network traffic.

On receiving a connection request to a port that can be used by a vulnerable service, (for examples, 80, 21, 23, 445, etc.), the plug-in will not consider it a single request, but as a number (X) of connection requests performed by the remote host, where X is the weight (importance) assigned to that port. A port's weight is a decimal value that indicates that port's vulnerability or likelihood of being used in an attack. A greater number indicates a more vulnerable port.

The weights of all ports to which requests were sent during a specified time interval are summarized and if this number exceeds the current port scan alarm level, a "Port scanning" alert will be displayed.

There is no way to determine with certainty if the computer is being port scanned (someone trying to see if there's a vulnerable port open). It is very much like having a stranger covertly glance at you several times. The question is how many glances (or ports scanned) before you start to become concerned. By setting the Attack Detection sensitivity you define the maximum number of attempts to connect to user's computer before the "Port scanning" alarm is triggered.

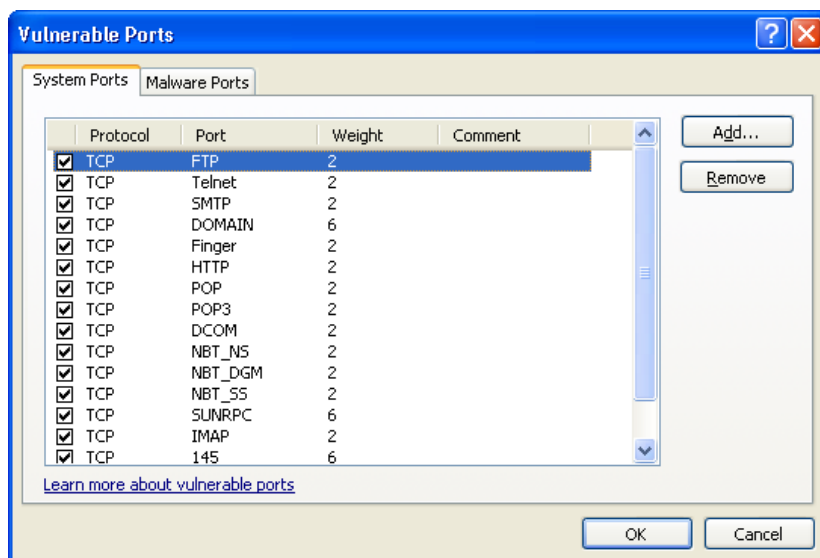
Example

Let the Attack Detection level be set to **Optimal**;
 Vulnerable port 80 weight is set to 7;
 Vulnerable port 21 weight is set to 3.

A "Port scanning" alert will be displayed if a remote host:

- Attempts to connect to the system's port 80 one time.
- Attempts to connect to the port 21 once and to any other port three times.
- Attempts to connect to any other ports on user's computer six times.

To specify a port that you consider vulnerable and to view the port weights, click **Customize > Advanced** and click **Specify** under **Vulnerable ports**. Unlisted ports have weights specified by the **Closed port weight** and **Open port weight** settings:



Vulnerable ports are divided in two groups: **system ports** and **malware ports**. Add ports that are used by vulnerable system services to the system ports list. Add ports that are exploited by well-known malware to the malware ports list. Select the tab according to the list you want to change.

To add a port, click **Add** and specify the following parameters: protocol, port number and weight. Weight is a decimal value that indicates that port's importance. A greater number indicates a more vulnerable port. You may also add optional comments in the corresponding field to describe the port's purpose or anything else you'd like noted.

Click **OK** to add the port to the list.

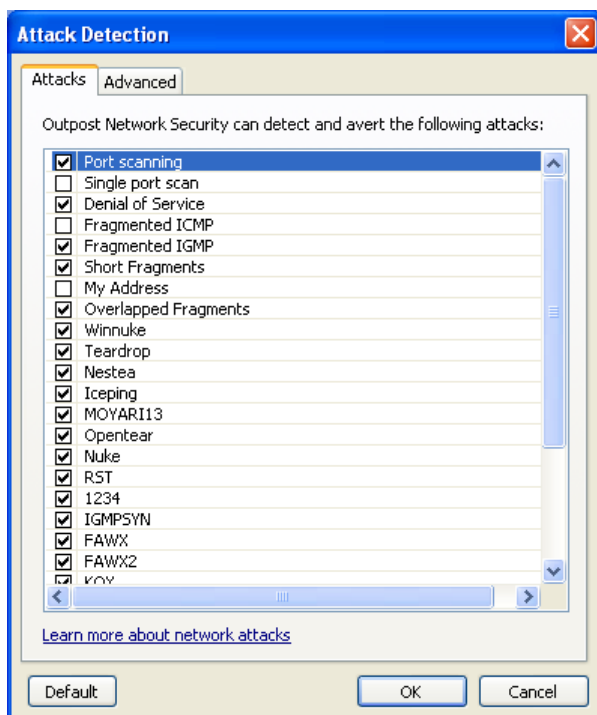
Note:

- To specify the time interval for detecting port scanning, edit the **Attack duration time** setting (**Customize > Advanced > Edit List > Advanced**).
- For additional information about ports that might be abused, see this article: <http://www.agnitum.com/support/kb/article.php?id=1000242&lang=en>.

Attacks List

You can designate the attacks Outpost Network Security is to detect and block. By default, more than 25 different types of attacks or exploits are handled, but you can select not to detect certain types to lower system resource usage or to stop too-frequent or faulty alert messages that may appear if, for example, a trusted service in your network is falsely perceived as an attack source.

To customize the attack detection list, click **Customize** and then **Edit list** on the **Advanced** tab:



All the selected types of attacks are detected by the firewall. To exclude a type, clear its check box. To revert to the default settings, click **Default**.

Note:

- For additional information about attack types, see this article: <http://www.agnitum.com/support/kb/article.php?id=1000193&lang=en>.

Specifying Trusted Hosts and Ports

There may be computers that you are absolutely sure are not a source of danger to user's system as well as ports on the system you are sure cannot serve as an intruder's backdoor. In other words, you consider any monitoring of these hosts and ports unnecessary and prefer to conserve system resources and performance by not monitoring them. The Attack Detection component features exclusion lists to which you can add hosts and ports you don't want to be monitored.

To add a host, a subnet or port to the trusted list, click **Exclusions**.

Specifying trusted hosts

On the **Hosts and Subnets** tab, click **Add** and in the **Select Address** dialog specify the format you wish to use to enter the network or host address. The following options are available:

- **Domain name.** For example, www.agnitum.com. An active internet connection is required for this because the IP address needs to be looked up over the internet. The IP address is saved along with the domain name you enter and it is this IP address that is used by Outpost Network Security.
- **IP address.** For example, 216.12.219.12.
- **IP address with subnet mask.** For example, 216.12.219.1 - 216.12.219.255.
- **IPv6 address.** For example, 2002::a00:1.

- **Macro address.** For example, LOCAL_NETWORK. For information on using macro addresses to specify local or remote host, see [Using Macro Addresses](#).

Type in the desired address in the format you selected (wildcards are allowed) and click **Add**. You can add several addresses in sequence this way and then click **OK** to add them to the trusted list. To remove an address from the list, select it and click **Remove**.

To disable detection of attacks from gateways, clear the **Check traffic from gateway hosts** check box. Specify all hosts and subnets you consider trusted and click **OK** to save the settings.

Specifying trusted ports

Select the **TCP Ports** or **UDP Ports** tab depending on the port(s) you are going to add to the trusted list. You can either enter the port number or port range, separated by commas, in the text box provided or select the required port from the list and double-click it to add it to the text box.

To remove a port from the list, simply erase its name or number in the text box.

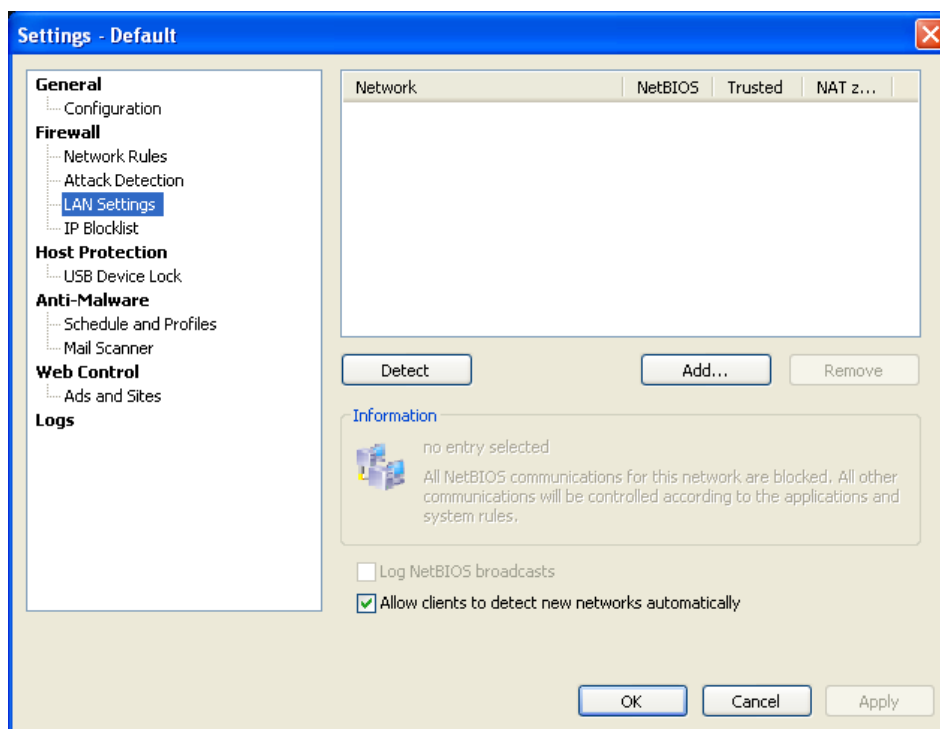
After specifying all the ports, click **OK** to save the settings.

LAN Settings

Outpost Network Security lets you [detect the networks](#) users' computers belong to and define the specific [access level](#) for each network.

Detecting a Local Area Network

You can use the **Detect** button to add networks to which your console belongs, if the client computers belong to those same networks. Otherwise, you should add the networks that the client computer belongs to manually by specifying the domain name, IP address, or IP range.



Note:

- LAN settings can be computer-specific and can be configured for a particular computer. For details, see [Monitoring Client Computers](#).

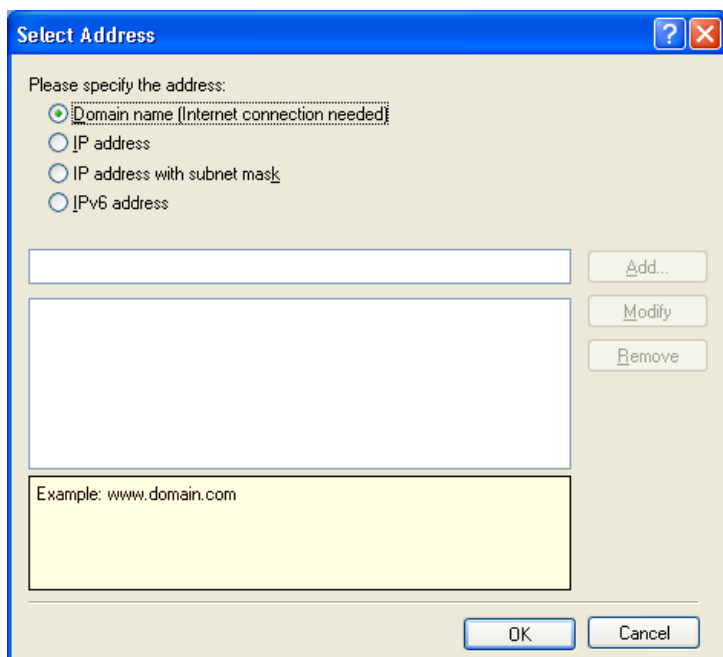
Detecting a LAN automatically

On the **LAN Settings** page, click **Detect** and Outpost Network Security will automatically discover the networks your computer belongs to and will create a list of their IP addresses, specifying the default level of access for each local detected network. You can then fine-tune the appropriate access levels for each network.

For Outpost Network Security to automatically detect new networks on client computers, so you do not need to add them manually, select the **Allow clients to detect new networks automatically** check box.

Adding a network address manually

If you prefer to manually add a network or remote host to the list and to configure a specific access level for it or if for some reason Outpost Network Security did not detect networks automatically, click **Add** and in the **Select Address** dialog specify the format you wish to use to enter the network or host address. The following options are available:



- **Domain name.** For example, www.agnitum.com. An active internet connection is required for this because the IP address of the domain name needs to be looked up over the internet. The IP address is saved along with the domain name you enter and it is this IP address that is used by Outpost Network Security.
- **IP address.** For example, 216.12.219.12.
- **IP address with subnet mask.** For example, 216.12.219.1 - 216.12.219.255.
- **IPv6 address.** For example, 2002::a00:1.

Type in the address in the format you selected (wildcards are allowed) and click **Add**. You can add several addresses in sequence this way and then click **OK** to add them to the list on the **LAN Settings** page. Configure the appropriate access levels for each network and click **OK** to save the settings.

Removing an address from the list

You can remove a selected address or network from the list by clicking the **Remove** button. Removing an address from the list is similar to specifying the **Limited Access to LAN** level for that address (i.e. clearing both the **NetBIOS** and **Trusted** check boxes).

Specifying LAN Access Levels

All computers on a LAN can be assigned one of the following levels of access regarding your computer:

- **NetBIOS** access: only File and Printer Sharing between the LAN and your computer is allowed. To set this level, select the **NetBIOS** check box for this address.
- **Trusted**: all connections to and from the network are allowed. To set this level, select the **Trusted** check box for this address.
- **NAT Zone**: select this check box, if you use internet Connection Sharing and other computers on the network get internet access via your computer.
- **Limited Access to LAN**: NetBIOS communications are blocked, all other communications are handled by application and global rules. To set this level, clear both the **NetBIOS** and **Trusted** check boxes for this address.

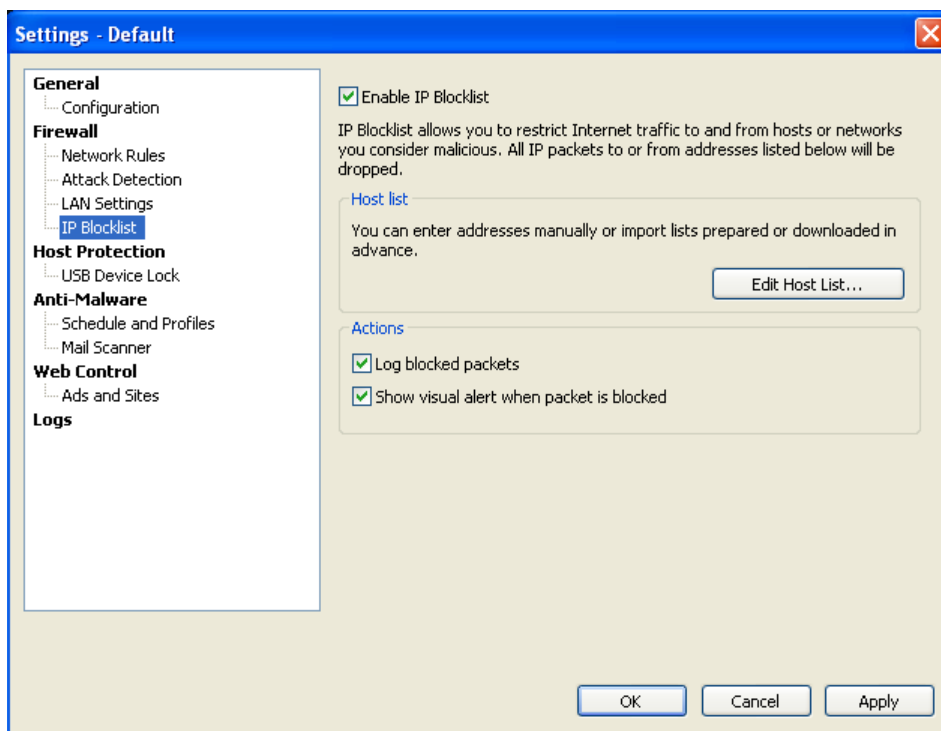
It is very important to remember that a host on a **Trusted** network is given the highest priority. Even restricted applications can communicate with the host. It is recommended to set *only absolutely trusted* computers as **Trusted**. If you just need File and Printer Sharing, use **NetBIOS** instead of **Trusted**.

If you do not want to clutter up logs with information about NetBIOS broadcast packets, you can disable data logging for all detected hosts and subnets by clearing the **Log NetBIOS broadcasts for detected networks** check box. This will keep the Event Viewer data clearer and may improve computer performance.

Note:

- NetBIOS broadcast packets are inbound or outbound UDP packets with the sender's address belonging to the selected subnet and sent to address 255.255.255.255 from port 137 or 138. Client computers commonly announce their presence on the network using such packets.
- Please note that Outpost Network Security's protective components are independent from the address access level. For example, even if you add www.agnitum.com to **Trusted** network addresses, its components will still block banners, active content, etc. from this site and perform their common activity regardless of the address access level.

IP Blocklist



Besides providing several different ways to block unwanted IPs—such as special firewall global and application rules—Outpost Network Security incorporates another tool to flexibly restrict unwanted traffic: **IP Blocklist**. Designed to filter out all inbound/outbound internet connections by IP addresses, this tool is essential for advanced users. It enables complete control over all user computers' network activity by blocking/denying specified IP addresses.

Outpost Network Security's IP Blocklist blocks hackers, malicious web sites, and advertising networks through the use of blacklists of IP addresses associated with each threat and annoyance. You can either compose your own lists of malicious IPs—even define a range of IP numbers that you consider unsafe—or search the net for free, easily available, predefined text-based lists. And, you don't have to spend time creating rules.

The IP Blocklist component is given maximum priority in Outpost Network Security's traffic processing algorithm, so its priority is even higher than that of trusted applications or of LANs marked as **Trusted**. No application, including the operating system itself, is able to send or receive basic IP or higher protocol data to or from a host in the IP Blocklist pool.

To enable IP Blocklist, select the **Enable IP Blocklist** check box.

Outpost Network Security is not shipped with a preset IP address list, but you can either download specialized or general lists from the internet or create them manually.

Outpost Network Security supports various list formats. To import a downloaded list, click **Import** on the **IP Blocklist** page, browse to the list file and click **Open**. The list is saved in the product configuration and can be imported or exported along with a full set of your settings if you change configurations. To save the current list as a separate file, click **Export**, select the folder to save the list into and click **Save**.

Note:

- Be sure to double-check the IPs before you add them to a list to avoid false positives, as some of the lists out there are quite old and IP addresses on them may have become legitimate.

To add an entry to a list manually, click **Edit Host List**, type in the address in one of the possible formats, specify a comment (so you'll know why you added the IP the next time you look at the list) and click **Add**. The entry will be added to the list. To delete an IP address from the list, select it and click **Remove**. To delete all the addresses from the list, click the **Remove All** button.

Formats of web addresses

There are four possible formats of addresses:

- **Domain name.** For example, <http://www.agnitum.com>. An active internet connection is required because the IP address needs to be looked up over the internet. The IP address is saved along with the domain name you enter and this is the IP address that is used by Outpost Network Security to block traffic.
- **IP address.** For example, 216.12.219.12.
- **IP address with subnet mask.** For example, 216.12.219.1/216.12.219.255.
- **IP range.** For example, 203.1.254.0-203.1.254.255.

Creating a blacklist manually

If you decide to create a list manually using a text editor, please note:

- Do not put spaces between any symbols.
- Specify the line number and separate it from the data with a comma.
- Comments start with the number sign (#).
- If you specify a subnet mask, place it immediately after the IP address with a slash between the address and mask.
- If you specify an IP range, use a hyphen.

The blacklist should have the following format:

- 1,IP/MASK#comment (an entry with a masked IP)*
- 2,IP1-IP2#comment (an entry with a range from IP1 to IP2)*
- 3,host,IP#comment (an entry with a DNS name)*

For example:

- 1,209.133.244.0/209.133.255.255#MEDIASENTRY-MEDIAFORCE*
- 2,203.1.254.0-203.1.254.255#ASIO*
- 3,hop.clickbank.net,209.81.0.46*

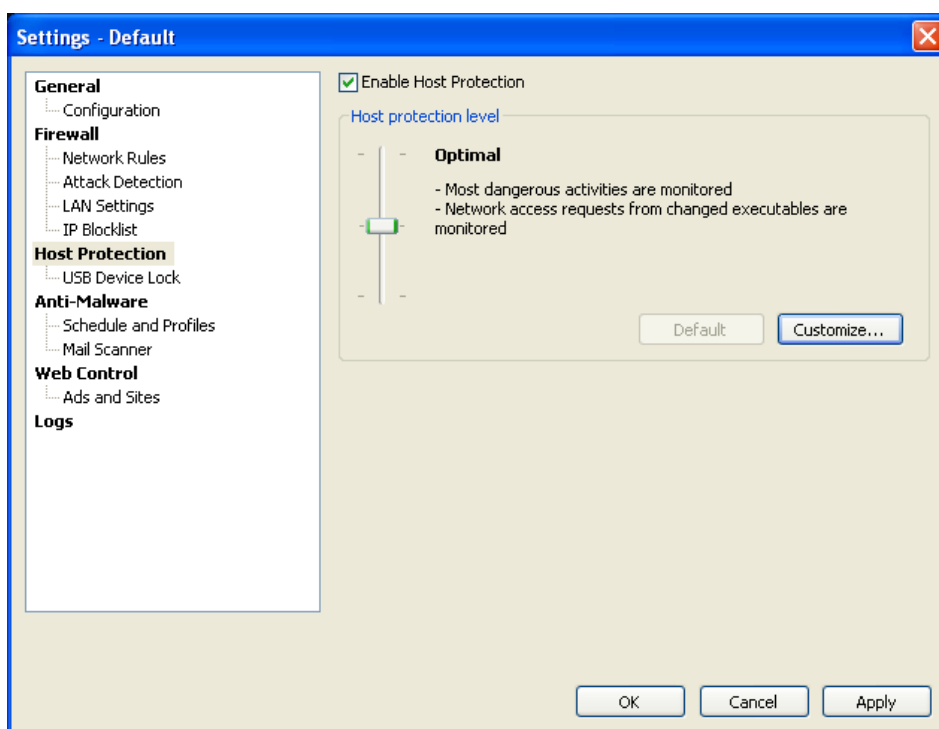
You can have Outpost Network Security log blocked packets and display visual alerts to users when packets are blocked by selecting the corresponding check boxes in the **Actions** section of the **IP Blocklist** page.

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 (such as browser) and thus gain the privileges needed to connect to the person who configured the Trojan. Others can start processes in hidden mode or hijack trusted process memory to pretend to be an application you do not consider harmful.

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

To enable Host Protection, select the **Enable Host Protection** check box:



It is not recommended to disable Host Protection. You might disable it when users experience significantly reduced performance, crashes, or other errors that lead to system instability and you want to verify that these instabilities are not being caused by Outpost Network Security. Turning Host Protection off severely reduces system's security level, as it is no longer having each system activity monitored.

Setting Local Security Level

The current degree of protection is characterized by the local security level setting which represents the combination of specific [Anti-Leak Control](#) and [Critical System Objects Control](#) settings providing the level of host security.

The following security levels are available:

- **Advanced.** Ensures protection against all penetration techniques that are often used by malicious software to bypass security software. Network requests from changed executables are monitored. The launching of changed executables is monitored. Changes of all critical objects are monitored.
- **Optimal.** Provides protection against the most dangerous penetration techniques. Network requests only from changed executables are monitored. Changes of all critical objects are monitored. If selected, some of the more exotic security test programs (leaktests) will fail.
- **Low.** If you select this option, Anti-Leak Control and Critical System Object Control are disabled completely. Only changed executables are monitored. This produces the minimal number of product prompts.

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 [Critical System Objects Control](#) according to your specific requirements.

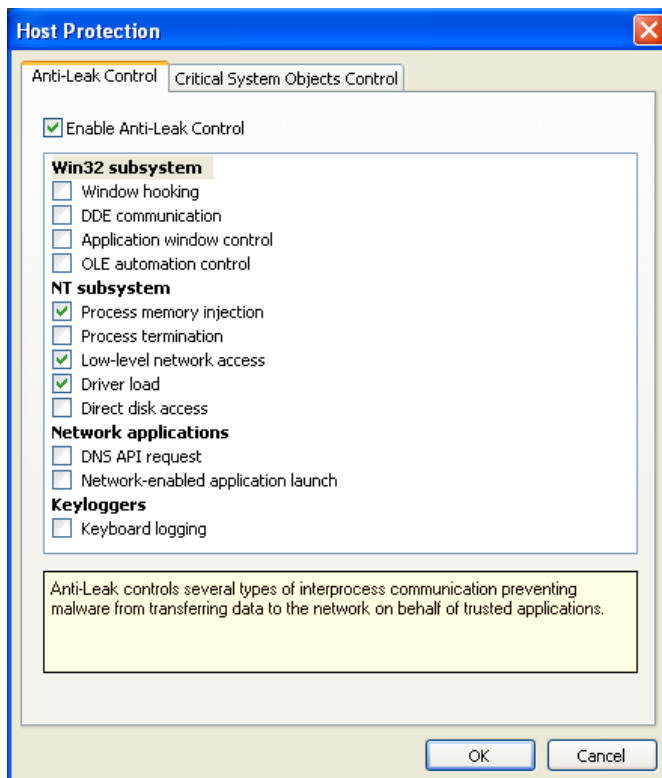
To restore the default security level, click **Default**.

Controlling Penetration Techniques

There are several advanced penetration schemes that allow malicious software to bypass the security perimeter of a PC. Outpost Network Security provides proactive security functionality called **Anti-Leak**

Control that blocks all currently-known penetration techniques that are often used by malicious programs to bypass security software (for details, see [Understanding Penetration Techniques](#)). This prevents sensitive data leakage from individual PCs, gives more control over what's happening on a PC, and alerts you to 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 the user's work.

To enable Anti-Leak Control, click the **Customize** button, and select the **Enable Anti-Leak Control** check box. All the techniques are divided into groups according to their types and possible actions within the system. The available settings allow you to select whether a technique should be controlled by Outpost Network Security or not. If you want the product to control a technique, select the check box next to it.



Note:

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

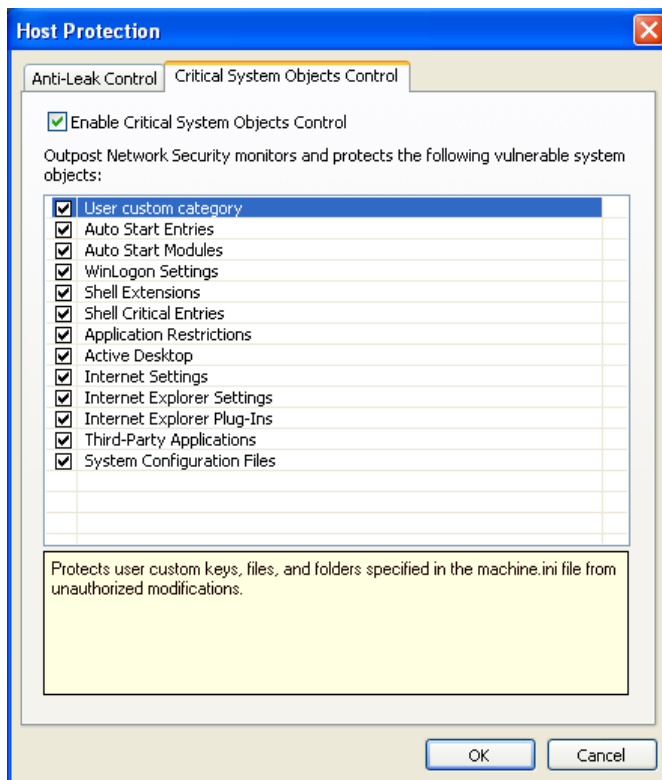
Controlling Critical System Objects

When you install any new software on the system, it registers its components in critical areas of the system registry. This is so the system does not interfere with a new program's performance.

Malware tends to register within critical system objects as well so it can freely perform its activities and arouse no suspicion within security products. Therefore, before starting its main activities of breaking system stability or security, malware tries to modify critical entries for its needs.

To prevent this, Outpost Network Security protects the most critically important system objects. It warns a user if any executable file tries to modify them and prompts for further action.

A list of critical system objects that are protected from malicious and accidental changes by various applications is available by clicking **Customize > Critical System Objects Control** tab:



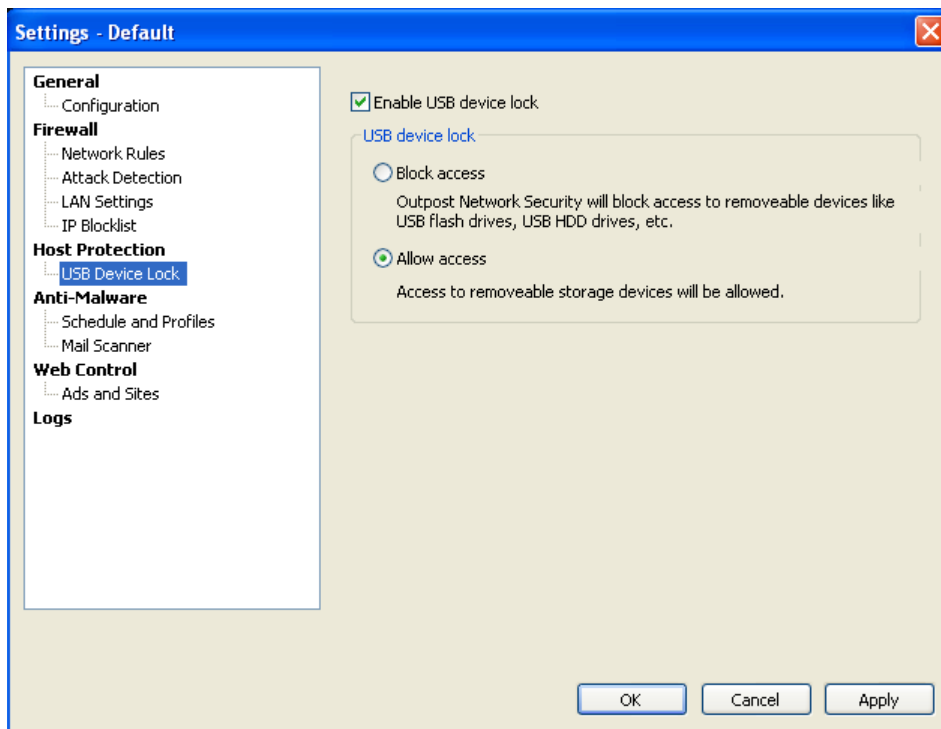
To learn more about each object, highlight it and you will see its description below.

To enable Critical System Objects Control, select the **Enable Critical System Objects Control** check box. If you do not want a particular object to be monitored by Outpost Network Security, clear its check box. You will always be able to restore the default settings at any time.

USB Device Lock

USB device lock allows you do block malicious code execution from removable USB drives preventing distribution of newfangled USB worms.

To enable USB device lock, select the corresponding check box and specify the policy according to which Outpost Network Security will control access to those devices.

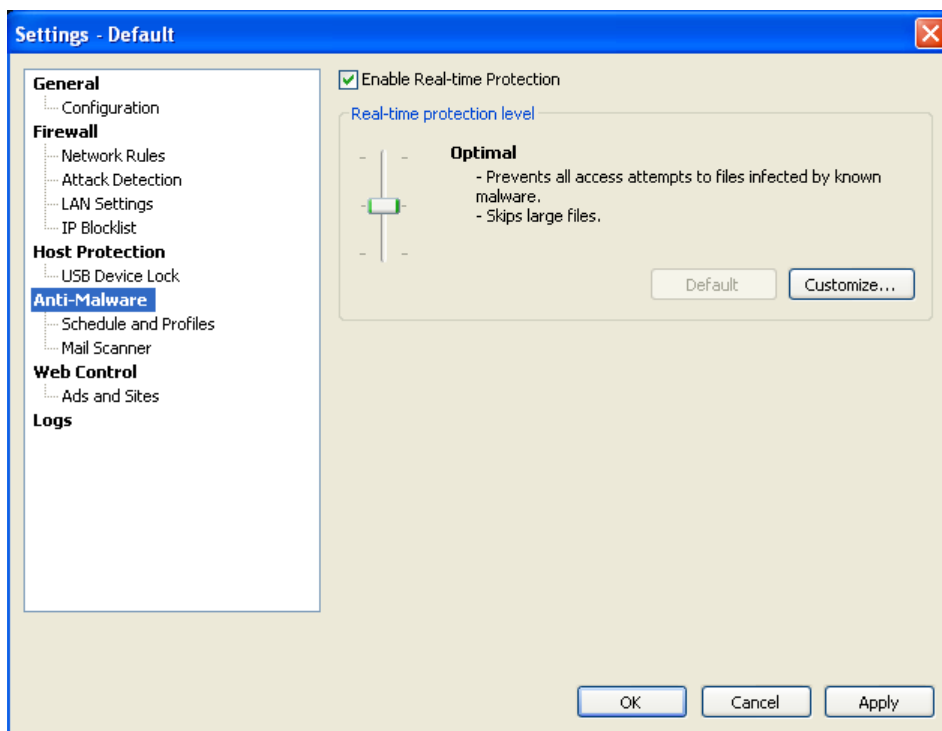


Anti-Malware

The Anti-Malware component is designed to prevent unwanted and unauthorized actions being performed by malware. Both antivirus and anti-spyware capabilities are provided through the universal component to ensure that your computer is kept clean of any malicious programs that might infect it while you're surfing the web or otherwise working.

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

To enable real-time protection, select the **Enable real-time protection** check box:



There are three levels of real-time protection possible to select:

- **Maximum.** All access attempts to files infected by known malware are prevented. Embedded OLE objects are checked either. A heuristic method of finding new malware is used.
- **Optimal.** Files are checked when they are accessed. Files larger than 20MB are skipped.
- **Relaxed.** Particular types of executable files are checked only when they are executed. Files larger than 20MB are skipped.

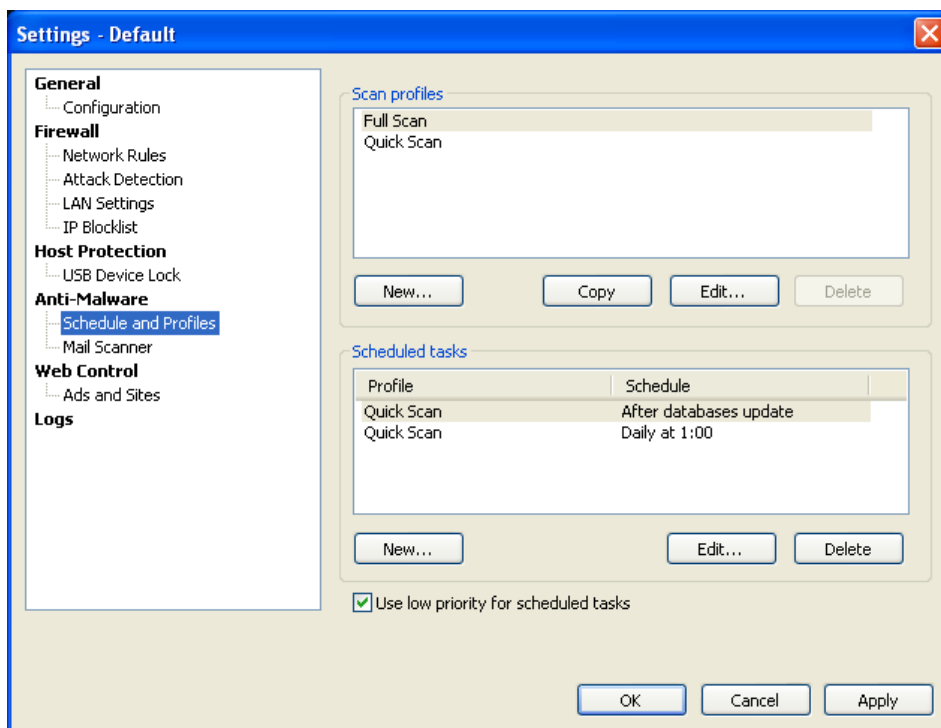
If you want to create your own real-time protection level, click the **Customize** button. In the dialog box you can set the real-time protection operation mode. Select **Check files on every access attempt**, which will prevent all access attempts to files infected by known malware. Note that this last mode can affect system performance. Or, you can select **Check files on execution**, if you want to prevent known malware from executing, but don't want to prevent other access attempts such as copying malware samples or displaying the contents of a folder where malware is located. Only file extensions that are on the **Extensions** list will be checked on any access attempt.

Tip:

- To improve scan performance, you can have Outpost Network Security create scan status cache files in each scanned folder by selecting the **Enable SmartScan technology** check box on the **General** tab of the product properties. Note, that the cache files are invisible and therefore may cause false positives from anti-rootkit tools.

Schedule and Profiles

Scheduling a system scan is a very useful option if you want to save time and user computer resources while scanning the system or if you need to perform regular scans. Outpost Network Security can perform scans in unattended mode when users are away of the computer.



By default, scheduled quick scans are performed after updating the malware database and daily at 1 a.m. To create a scheduled scan, click **New**. Enter a name for your task, select a scan profile to be used from the drop-down menu and specify the scan schedule. To create regular malware scans, use the **How often** list. If you select **Weekly** scanning, you can also specify the day and exact time when Outpost Network Security will scan your system. If you choose **Daily** scanning, you can specify the time of day for the scanning to begin.

To temporarily disable a scheduled task without deleting it, highlight it on the list and click **Edit**. Clear the **This task is enabled** check box. The profile is not permanently deleted, and later you can enable it again. To delete a profile completely, highlight it and click **Delete**.

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

Creating a scan profile

A scan profile is a set of predefined scan settings to be applied and used during a system scan. Having created a scan profile with settings that suit your requirements, you relieve yourself from the need to specify the same settings each time you want to perform a scan. Instead, you simply select the profile name from the list and all the settings stored in that profile are used to scan your system.

To create a new scan profile, under **Scan Profiles** click **New**. In the dialog box, give a descriptive name to your new profile and click **OK** to continue.

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

Each profile can be edited or removed (except the default **Full Scan** and **Quick Scan** profiles) any time later by clicking the corresponding buttons.

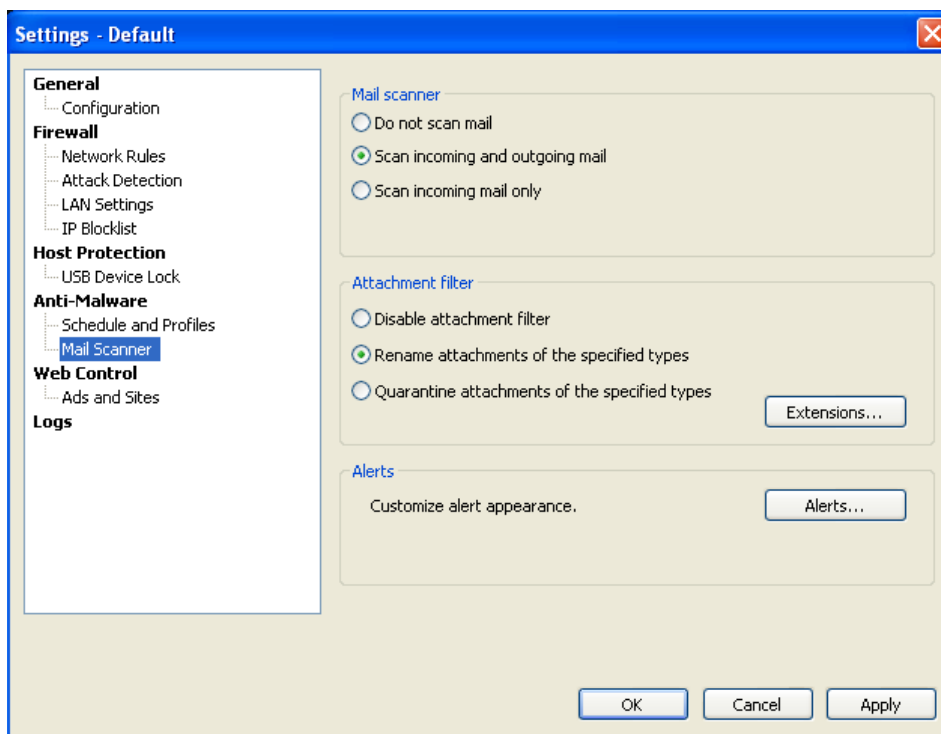
After selecting the scan type and, if necessary, the scan profile name, click **Next** to proceed.

Mail Scanner

One of the simplest ways for worms, Trojans, and other malware to get into user's computer is through e-mail attachments. Hundreds of self-replicating programs use e-mail and address lists of unlucky users to distribute themselves throughout the internet and/or a local network. A user needs only to open the

file attached to a received e-mail and the worm or virus starts performing its malicious actions resulting in system infection and malfunction.

Outpost Network Security protects users from attachments containing viruses, worms, and Trojans, checking files attached to e-mail arriving to and being sent from the computer and quarantining those which Outpost Network Security recognizes as potentially dangerous:



Under **Mail scanner** you can select which mail will be scanned: both incoming and outgoing mail or incoming mail only according to your needs. Also specify the action to perform on malware that is detected in your e-mail by selecting **Cure** or **Quarantine** in the **When malware found** list.

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

Attachment filter

If you consider some types of attachments to be potentially dangerous even after they pass a clean malware check (for example, the scanner could simply be not "aware" of 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 a file.

The attachment filter is triggered after clean malware scan quarantines or removes specified types of files according to the settings under **Attachment filter** on the **Mail Scanner** page.

Select **Rename attachments of the specified types** if you want to change the extension of the file or **Quarantine attachments of the specified types** to isolate them and put them in Outpost Network Security's quarantine.

To edit the list of file extensions to process, click the **Extensions** button. The most common types of files that can contain malicious code are already added to the list for your convenience, but you can add, edit, or remove file extensions according to your needs. To revert to the original list, click the **Default** button.

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

You can also set Outpost Network Security to show visual alerts and/or play sound alarms on detecting malware by clicking the **Alerts** button under **Notifications**.

Note:

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

Web Control

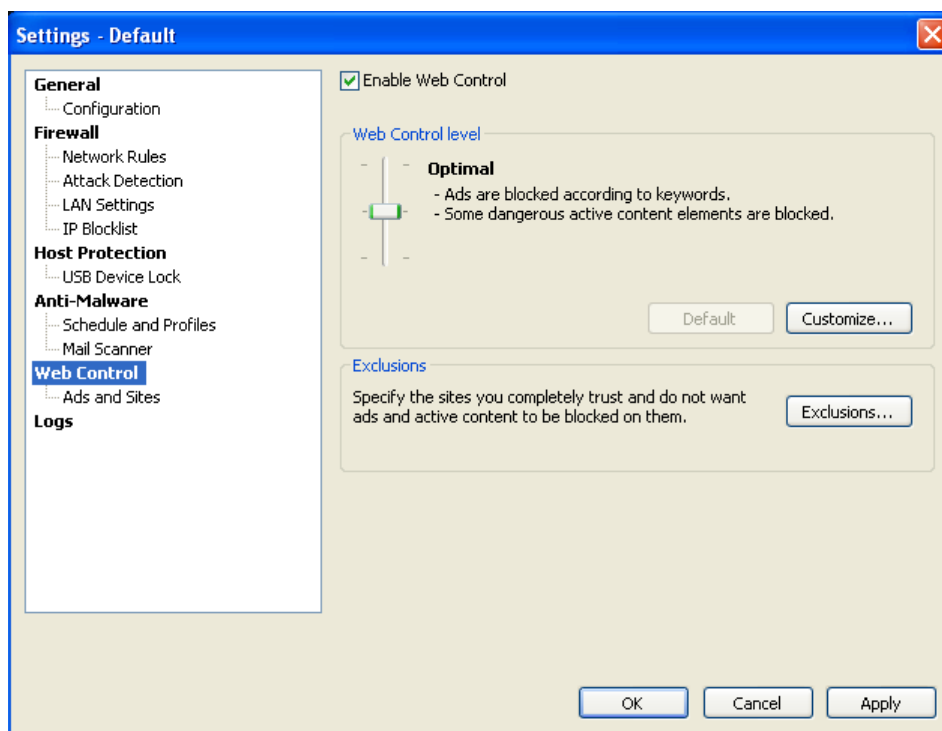
Contemporary web site developers embed active elements in web pages to extend their functionality, increase user interactivity and improve web site usability. These elements include ActiveX, Flash, JavaScript, VBScript, and others. These technologies were developed to improve the user experience as people browse web pages, but hackers are now successfully using them to gain control of user's computer. Active elements can pose a security risk to your system. Many sites also use them to display obtrusive, offensive or simply annoying ads, which can significantly decrease browsing speed.

Besides, more and more web sites are full of banner ads that often are very irritating, clutter up web pages with objectionable images and which can practically stop already slow modem browsing.

Outpost Network Security's Web Control component provides internet surfing safety. It controls the operation of active elements embedded in the web pages users are browsing or in the e-mail they are receiving so you can independently allow or block any of these elements. The following are controlled by this plug-in: ActiveX, Java applets, programs based on Java and Visual Basic scripts, cookies, pop-up windows, ActiveX scripts, external active content, referrers, hidden frames, animated GIF images, flash animations.

Web Control also blocks the display of banner ads from specific advertisers, which speeds up web pages. Advertisements can be blocked using two criteria: by keywords found in the content of the downloaded web page or by the size of the ad image.

To enable protection from such unnecessary ads and active content, select the **Enable Web Control** check box:

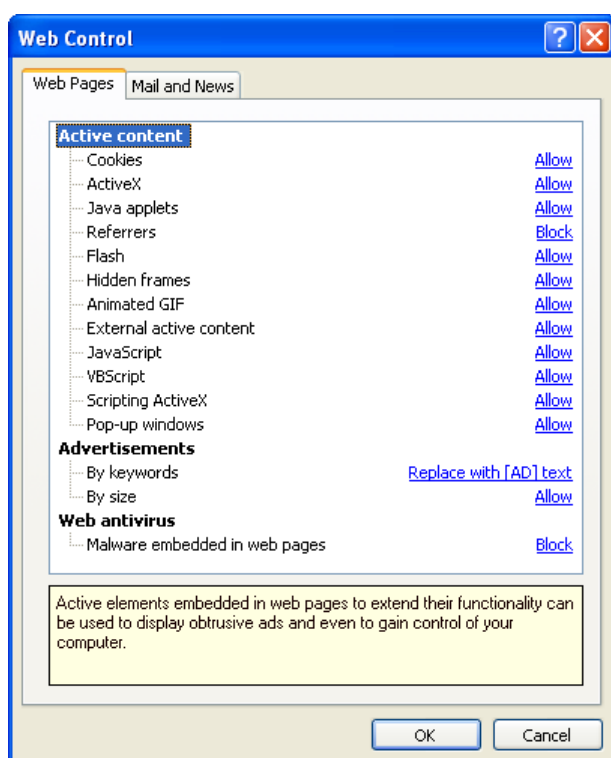


Setting Web Control Level

You can specify how thorough Outpost Network Security should be in processing web content by changing the Web Control level. The following levels are available:

- **Maximum.** Advertisements are blocked according to specified keywords and sizes. The most dangerous active elements are blocked or cause a prompt to be displayed to a user.
- **Optimal.** Ads are blocked according to specified keywords and most active content elements are allowed.
- **Relaxed.** Ads are blocked according to specified keywords and all active content is allowed.

If you want to define special settings, you can customize the protection level. Click the **Customize** button and the displayed window will let you independently configure the treatment of interactive elements and ads contained in downloaded web pages or user's e-mail and news:



Go to either the **Web Pages** or the **Mail and News** tab and select the element type to manage. The bottom part of the window will show you the element description. To allow or block a particular element, click the keyword of the action. You can select one of the available options:

- **Allow.** All elements of this type are always allowed.
- **Prompt.** Outpost Network Security prompts you before allowing an element of this type.
- **Block.** Elements of this type are always blocked.

For advertisements, Outpost Network Security gives you the option to either replace banner ads with text "[AD]" or with a transparent image the same size as the banner. Note that although replacing banner ads with transparent images greatly increases your comfort level while browsing by removing annoying graphics, you may prefer to replace banners with the "[AD]" text links so users can still use the links if you like.

Click **OK** to save the new settings.

The **Default** button restores the default protection level.

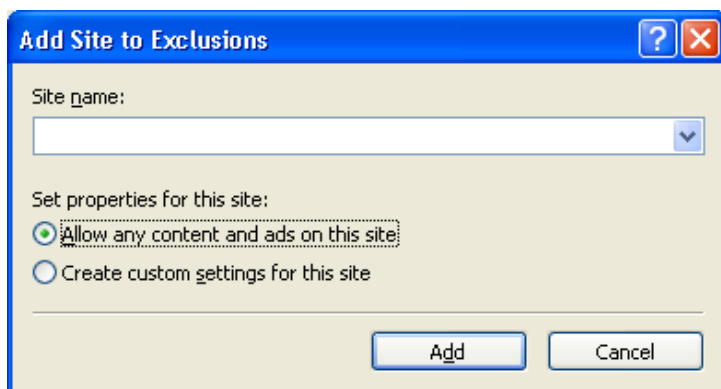
Note:

- The **Prompt** option is not available for hidden frames, animated GIFs, and external active content.
- 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: necessary 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 regularly visited sites, just change these settings for those sites by adding them to the [exclusions list](#); otherwise you may need to loosen the default web content treatment policy.

Specifying Exclusions

If users experience problems viewing specific sites because most of the site's images are filtered out, you can add those sites to the exclusions list and set the policy for handling active content elements and ads individually for that particular web site to stop the component from being blocked.

Click **Exclusions** and click **Add** to specify the address of the site you want to personalize the content settings for:

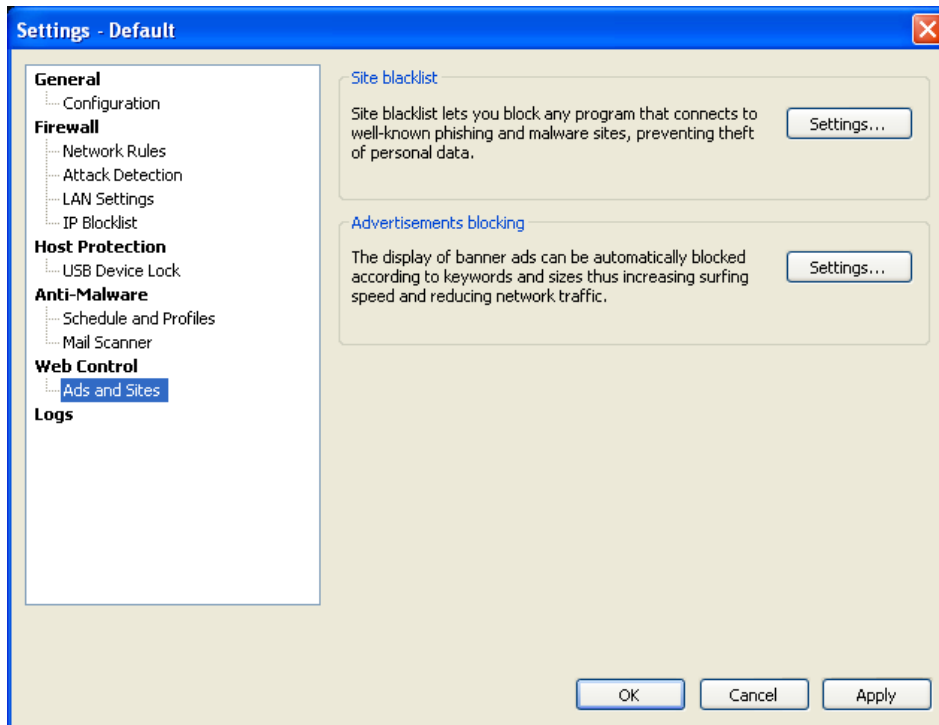


You can either **Allow any content and ads on this site** making it completely trusted or specify your individual settings by selecting the **Create custom settings for this site** option. In the second case, after clicking **Add** the **Edit Properties** window for this site will be displayed allowing you to set how the site's active content and ads should be treated. The site that you add is immediately given all the default active content and advertisement settings for the current Web Control level. The settings are pretty much the same as the [global settings](#) for all sites. The only difference is that you can select the inherited global value (for the active elements—instead of the **Prompt** action) for the element behavior to be defined by the global setting (marked with asterisk) for this site.

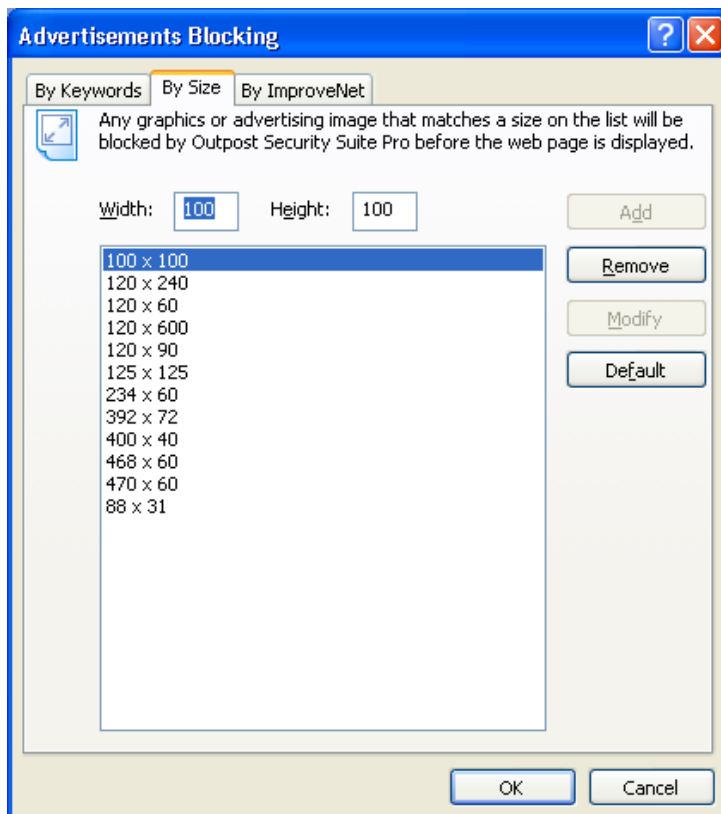
Make your choices (use the **Default** button if you want to start from the global settings again) and click **OK** to save your changes.

You can later edit the site's active content and ad settings by selecting the site from the list and clicking **Properties**.

Ads and Sites



Advertisements can be blocked using the following three criteria: by keywords found in the content of the downloaded web page, by size of the advertising image and using the data collected via the Agnitum's ImproveNet program:



Blocking by keywords

Outpost Network Security blocks ads basing on keywords found in internet advertisement URLs located in the "*IMG SRC=*" and "*A HREF=*" HTML tags. If the banner URL contains one of the specified keywords, it is replaced with the text "*[AD]*" or with a transparent GIF image the same size as the ad image.

To open the component's list of keywords, click **Settings > Ads and Sites > Edit List**. To add a word to the blocked list, type it in the provided text box and click **Add**. The word will appear in the list and any advertisement that contains this word, will not be displayed in the web browser. You can also edit and remove keywords from the list.

You can also import and export lists of keywords by using the corresponding buttons.

Blocking by image size

Outpost Network Security blocks advertisement images based on their size as specified within the "*A*" HTML tag. If the banner size matches one of the sizes on the list, it will be replaced with the text "*[AD]*" or with a transparent GIF image of the same size.

By default, the standard size ad images are already on the list. To block a banner with a different size, click **Edit List**, select the **By Size** tab and specify the banner's width and height in the fields provided and click **Add**. The size record will appear in the list and any ad of this size will not be displayed in the web browser. You can also edit and remove sizes from the list. To reset the list to its default state, click the **Default** button.

Blocking by ImproveNet

This function is similar to "blocking by keywords" with the difference that the keywords in ImproveNet *are shared by users of Outpost Network Security*. The list of ImproveNet keywords is automatically updated along with the regular product updates either automatically (if that is your preference) or manually.

Blocking by ImproveNet is an optional function, therefore if you do not need it you can disable it by clearing the **Use ImproveNet ads keyword list** check box on the **ImproveNet List** tab.

Note:

- Banner ads are blocked according to the settings you specify. Therefore, some legitimate images could be blocked if a setting is too broad, such as adding the word "image" to the list of keywords. At the same time, some ads might not be blocked with the component's default settings.

Site Blacklist

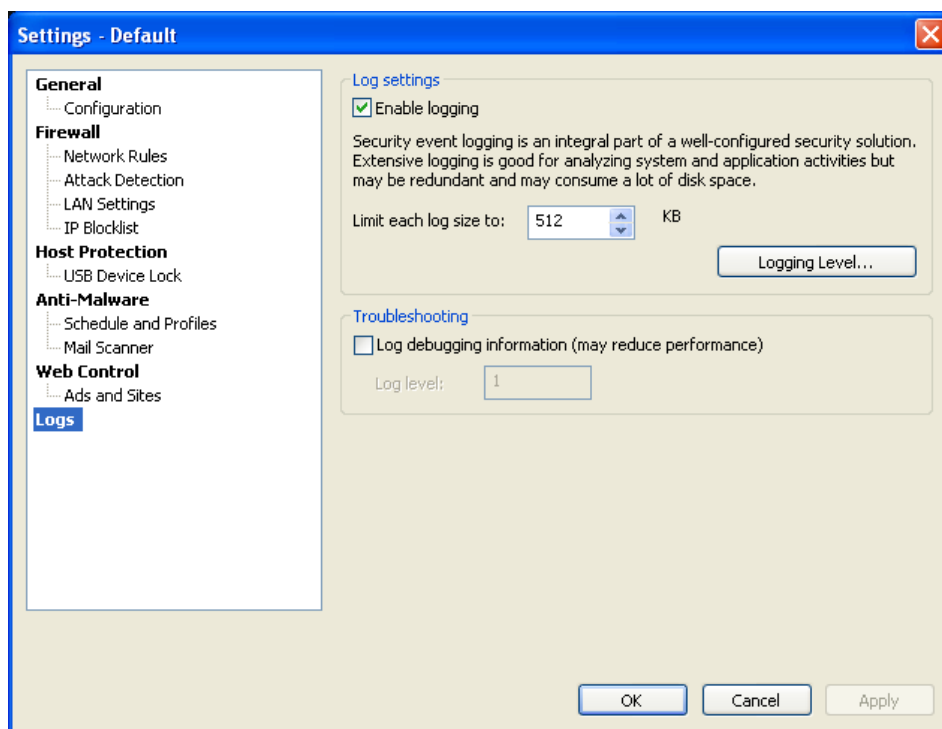
Various sites on the internet contain spyware and they aim at spreading it among unwitting users. Outpost Network Security's database contains a list of such sites, access to which is not recommended unless user is eager to load spyware on his system on purpose. An attempt to make a connection to such site or to send any data there is automatically blocked.

To enable spy site blocking, select the **Enable spy sites blocking** check box. For the user to be aware of blocking events, you can set Outpost Network Security to display alerts by selecting the **Show visual notifications** check box.

Also, you can create your own custom list of spy sites on the **Custom List** tab of the **Site Blacklist** window.

Logs

To be able to get more information about user systems' activity in case they encounter some issues with how specific applications perform, you can increase the depth of logging of firewall events or even enable logging of debugging information which can be useful for Agnitum technical support service engineers to be able to resolve your issues.



Firewall logging level

To set the detail of firewall logging, click **Logging Level**. You have the ability to set the level of your global system logging and of application events, as well as low-level events.

Logging debugging information

To enable the logging of additional debugging information that is required for Agnitum's technical support service, click **Settings** on the toolbar, select the **Logs** page and select the **Log debugging information** check box. This will extend the number and detail of logged events.

You can modify the detail of which debugging information is logged by changing its logging level from 1 to 4. For the level change to take effect, you need to restart Outpost Network Security.

Note:

- Increasing the logging level may reduce user systems' performance.

Tip:

- The size of each log can be limited to prevent log overgrowth and to save your hard disk space. Under **Log settings**, you can specify a size limit for every log in kilobytes.

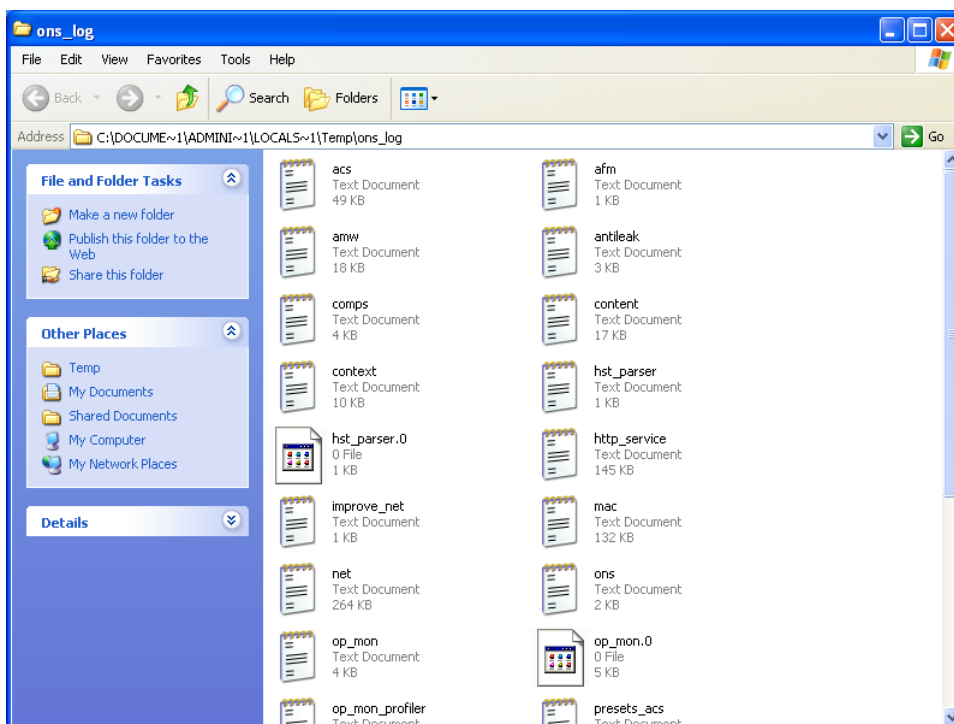
Monitoring Client Computers

To monitor client computers remotely, Outpost Network Security provides the following functionality available through the computer's shortcut menu:

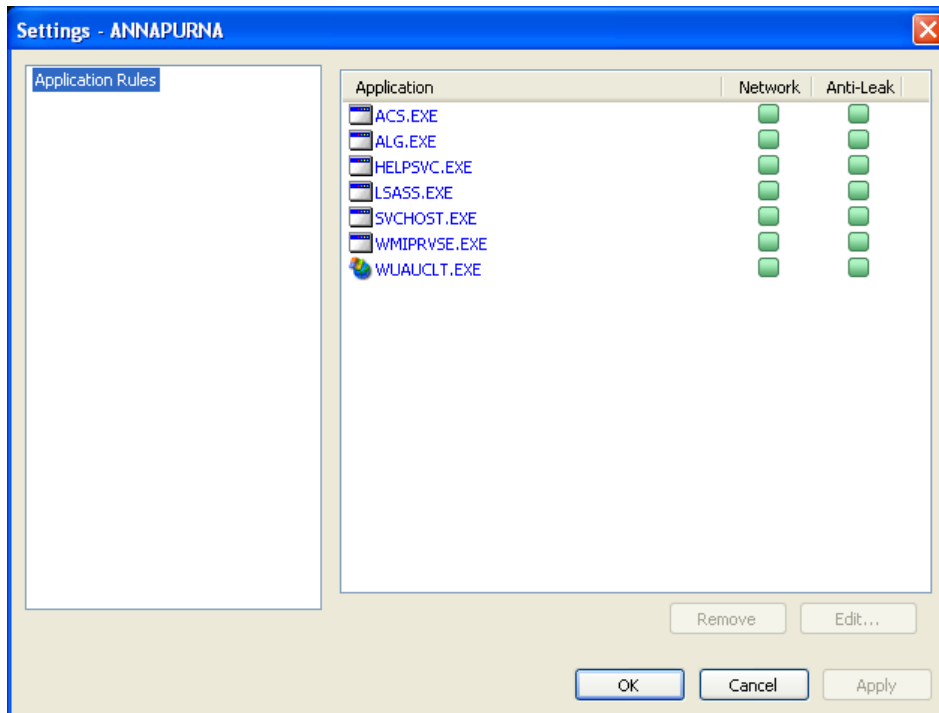
- Right-click computer's name and click **Open Remotely**. Outpost Network Security Client interface will be opened allowing you to perform any actions you would perform when you visit that computer – view logs, track online computer activity, modify application rules and LAN settings, etc.



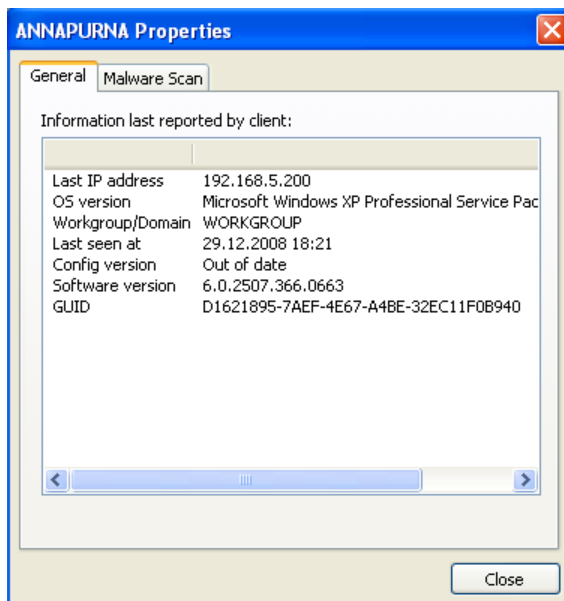
- To be able to view remote computer logs in text format, select **View Logs**. Log files from the client will be copied into temporary folder on the console and available for review in any text editor.



- To be able to view and manage computer application rules and/or LAN settings, select **Settings**.



- To view general computer information and malware scan details, select **Properties**.



Managing Groups of Computers

After being registered on the console, all the client computers are placed in the **Default** group. If you need to assign different security settings to different sets of computers, you can combine client computers into groups depending on the required settings and specify custom settings for each group.

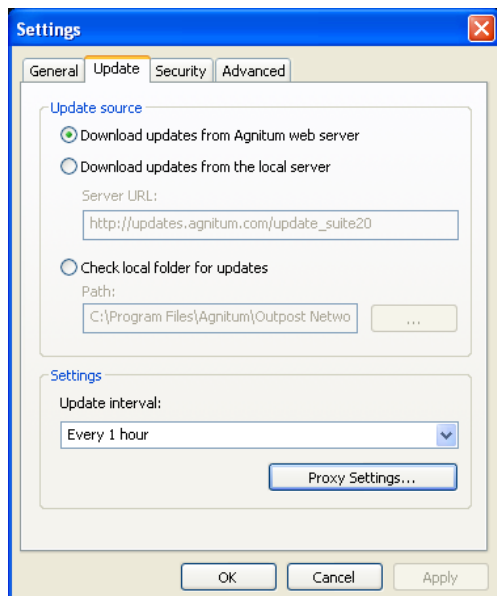
To create a new group, right-click the **Protected Computers** node and select **Add Group**. The new group will be created. Click **Rename** and specify the name for the group. If you want the initial settings for this group to be set based on one of the existing groups, right-click the existing group, select **Copy Settings to** and select the newly created group. To set the default settings, use the **Set Default Settings** command in the group's shortcut menu.

After the group is created, you can populate it with computers from other groups by using the **Move to Group** command on the computer's shortcut menu. All the clients will get the configuration set for the destination group.

Configuring Updates for Client Computers

By default, updates are downloaded by the console on an hourly basis, however, you can choose updates frequency on your own. To do this, click the **Settings** button on the toolbar, select the **Update** tab, and set the required update period.

You can also specify the source to take updates from. Under **Update source** select either Agnitum web server, local updates server (if configured), or folder where downloaded updates are centrally stored.



When the updates are enabled, they are automatically downloaded hourly, transferred to each client on their request and applied.

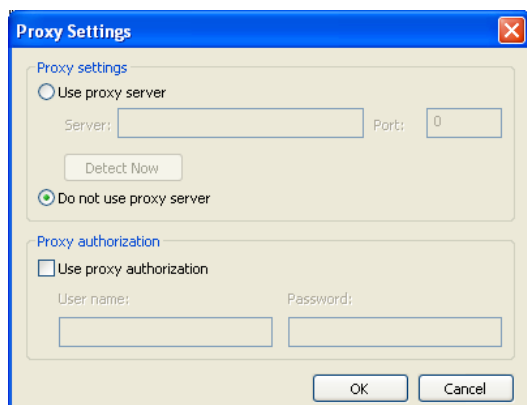
Configuring Connection Options

If you connect to the Internet through a proxy server, you can set the connection settings by clicking **Proxy Settings** on the **Update** tab. To specify the server and port number manually, select the **Use proxy server** option under **Proxy settings** and type in the server name and port number in the text boxes provided.

To autodetect the proxy server parameters, click **Detect Now**.

Along with specifying the proxy server, you can define whether it requires authorization by selecting the **Use proxy authorization** check box under **Proxy authorization** and specify the access credentials (user name and password).

If (when connecting to the Internet) your computer uses a proxy server, but you want the updating process to be performed directly from the product developer's server or you do not use a proxy server at all, select **Do not use proxy server**.

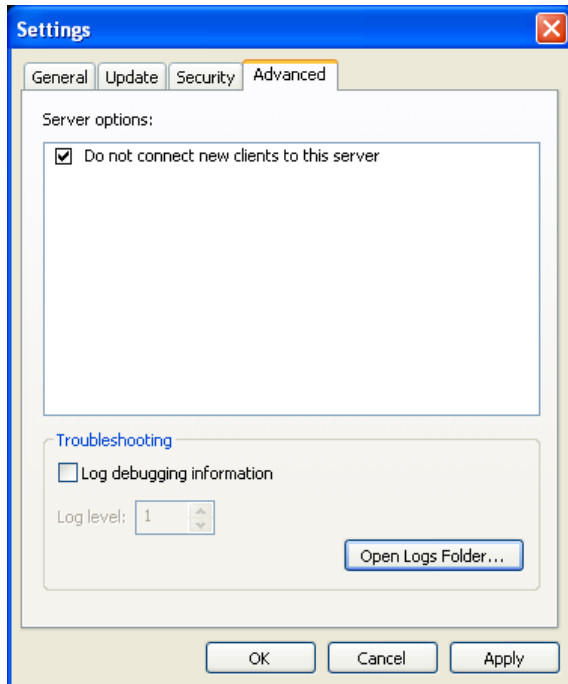


Server-Side Logging

You can enable server-side logging by selecting the **Log debugging information** check box on the **Advanced** tab of the **Settings** dialog in case you have any issues regarding the console operation. This will extend the number and detail of logged events.

You can modify the detail of which debugging information is logged by changing its logging level from 1 to 4. For the level change to take effect, you need to restart Outpost Network Security.

The collected information can be provided to Agnitum support service and will be helpful in resolving your problems.



Appendix

This appendix contains several technical topics, which can be useful for administrators to be able to better understand Outpost Network Security's internals.

Troubleshooting

If you need assistance in working with Outpost Network Security, please visit the Agnitum support page at <http://www.agnitum.com/support/index.php>. Among available support options are the knowledge base, documentation, support forum, product-related web resources, and direct contact with support engineers.

Understanding Penetration Techniques

By means of [Anti-Leak Control](#), Outpost Network Security allows you to control a lot of suspicious actions. For your convenience they are divided into 4 groups:

Win32 subsystem

Components injection

Windows operating systems by design enable installing system interceptors (hooks) through which foreign code can be injected into processes. Normally, this technique is used to perform common, legitimate actions, such as switching the keyboard layout or launching a PDF file within the web browser window. However, it can also be used by malicious programs to embed harmful code and thus hijack the host application. An example of a leak test that uses such a technique to stage a simulated attack is the PC Audit program (<http://www.pcindernetpatrol.com/>).

Outpost Network Security 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, such as internet Explorer or Firefox. The behavior of a DLL file invoking such functions is considered suspicious and triggers a legitimacy verification.

Control over another application

DDE technology is used to control applications. Browsers are commonly DDE servers, so can be used by malicious programs to transfer private information onto a network. One example of this technique is the Surfer leak test (<http://www.firewallleak tester.com/leak test15.htm>). ZABypass is another example of a leak test that uses this method.

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

Application window control

Windows allows applications to exchange window messages between processes. Malicious processes can gain control over other network-enabled applications by sending them window messages and imitating user input from the keyboard and/or mouse clicks. An example of using this technique is the Breakout leak test (<http://www.firewallleak tester.com/leak test16.htm>).

The crucial point here is program interactivity through the SendMessage, PostMessage API, and so on. This technique is used for legitimate inter-process interactivity, but can very easily be used for nefarious purposes by malicious individuals.

Outpost Network Security controls such attempts.

OLE application control

A relatively new technique has surfaced that controls application activity through OLE (Object Linking and Embedding) - a Windows mechanism, which allows one program to manage the behavior of another program on the computer. It uses the technique of OLE intercommunication to exchange data and commands between applications, for example, to manage the activity of internet Explorer so it can send user-specific data to a remote location. An example of using this technique is the PCFlank leak test (http://www.pcflank.com/PCFlankleak_test.exe).

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

NT subsystem

Process memory modification

Several Trojan horses and viruses use sophisticated techniques that let them alter the code of trusted applications running in memory and thereby bypass the system security perimeter in order to perform their malicious activities. This is known as code injection or copycat vulnerability. Examples of using this technique are the Thernite and Copycat leak tests (http://www.Antivirusleak_tester.com/leak_test8.htm, http://www.Antivirusleak_tester.com/leak_test9.htm).

Outpost Antivirus Pro enables you to control the functions that can be used to write malicious code into a trusted application's address space and so prevent a rogue process from injecting their code into those processes. The entire memory space used by any active application on a computer is monitored by Outpost Antivirus Pro (not just that of a network-enabled application). If malware tries to modify a legitimate application's memory, Outpost Antivirus Pro detects it and displays a pop-up alert. The system works proactively: it allows you to permit or deny the modification of memory of other processes at the application level. For example, Visual Studio 2005 would be able to modify memory, while the "copycat.exe" leak test would be disallowed from doing so. This feature protects against even unknown malware not yet detected by antivirus and anti-Malware vendors that exploits this vulnerability.

Process termination

Any legitimate process can be forcibly terminated in an unexpected manner by using debugging APIs. An example of using this technique is Comodo Leaktest Suite (<http://personalfirewall.comodo.com/cltinfo.html>; Injection: AdvancedProcessTermination method).

Outpost Network Security controls process termination attempts.

Low-level network access

Some network drivers allow direct access to the network adapter, which bypasses the standard TCP stack. These drivers can be used by sniffers and other malicious programs to get low-level network access. They pose an additional risk for the system as traffic passing through them cannot be screened by a Antivirus. The example of using this technique is MBtest leak test (http://www.Antivirusleak_tester.com/leak_test10.htm).

Outpost Antivirus Pro allows the control of applications that request non-standard network access. This feature strengthens overall network security level by preventing outbound data leakage. The user is able to control an application's attempts to open a network-enabled driver; so without the user's authorization, an application is not able to send even the ARP or IPX data.

Driver load

Applications working under the superuser account can install kernel-mode drivers in order to get complete and unlimited access to the system and work on its behalf. This might be necessary to hide their presence within the system or disabling security systems. An example of using this technique are various kernel-mode rootkits.

Outpost Antivirus Pro controls attempts to install drivers and checks each driver file against its malware database before the driver is loaded into memory. If used carefully, this technique is 100% effective protection against rootkit installations on the system.

Direct disk access

Any legitimate process can be forcibly terminated in an unexpected manner by using debugging APIs. An example of using this technique is Comodo Leaktest Suite (<http://personalfirewall.comodo.com/ctinfo.html>; Injection: AdvancedProcessTermination method).

Outpost Network Security controls process termination attempts.

Network applications

DNS query submission

The DNS Client service contains a vulnerability called DNS tunneling. Malicious code can transfer and receive any information using correct DNS packets to a correctly configured operating DNS server. An example of using this technique is the DNSTester leak test (<http://www.klake.org/~jt/dnshell/>).

Outpost Network Security performs double verification of any access to a DNS Client service, thereby providing a more secure system. This controls access to a DNS API even with the DNS Client service on, and thus benefits users who, out of compatibility concerns, cannot disable this service themselves. This functionality allows the assignment of permissions to a specific process to use the DNS Client service.

Network-enabled application launch

Malicious processes can launch your default web browser with command-line parameters (for example, 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 it to who actually launched it in the first place and what additional connection parameters are supplied, are unable to challenge the technique, and thereby allow confidential data to be transmitted from the computer. Examples of this technique are used by the Tooleaky, Ghost and Wallbreaker leak tests (http://www.firewallleak_tester.com/leak_test2.htm, http://www.firewallleak_tester.com/leak_test13.htm, http://www.firewallleak_tester.com/leak_test11.htm).

Outpost Network Security watches every program started on a computer and controls who has permission to start each program with command line parameters protecting your browser against tampering. Beyond browsers, command-line launch control applies to all network-enabled applications, which are present in the configuration. Outpost Network Security will prompt the user as to whether such activity should be permitted for a particular program.

Keyloggers

Keyboard logging

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

Using Macro Addresses

Outpost Network Security 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 Network Security automatically recognizes current macro values so you do not need to change host and subnet addresses whenever network adapter settings are changed. For example, a mobile user's protection will always be active since the rules on his laptop work regardless of what network he is connected to.

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

DNS_SERVERS

Specifies addresses of all DNS servers in your network.

LOCAL_NETWORK

Specifies addresses of all your local networks and addresses from the broadcast ranges available on your computer.

WINS_SERVERS

Specifies addresses of all WINS servers on your network.

GATEWAYS

Specifies addresses of all gateway servers for your network.

MY_COMPUTER

Specifies all IP addresses your computer has in different networks, including loopback addresses.

ALL_COMPUTER_ADDRESSES

Specifies all IP addresses your computer has in different networks, including broadcast and multicast addresses.

BROADCAST_ADDRESSES

Specifies addresses within broadcast ranges available to your computer. A broadcast address is an IP address that allows information to be sent simultaneously to all machines on a given subnet.

MULTICAST_ADDRESSES

Specifies addresses in multicast ranges. A multicast address is a single address that refers to multiple network devices. "Multicast address" is synonymous with "group address".

About Agnitum

Agnitum Ltd. is a software development company committed to delivering and supporting high quality security software products. Agnitum offers two headline products - Outpost Security Suite PRO, securing personal and family desktops, and Outpost Network Security, ensuring a reliable endpoint protection and performance of the corporate network. Agnitum delivers computer security solutions to large enterprises, small and medium businesses, as well as home PC users.

North America Sales Office:

130 El Bosque Ave.
San Jose, CA 95134

HQ address:

Acropoleos Avenue
8 Mabella Court
Nicosia, Cyprus