

Administrator

Guide

Reference

Outpost Office Firewall

Office Firewall Software

from

Agnitum

Abstract

This document provides information on deploying Outpost Office Firewall in a corporate network. It also describes the general process of configuring client firewalls.

For details on configuring client firewalls, please see the **Outpost Client Firewall User Guide**.

Table of Contents

Introduction	4
System Requirements	5
Components	5
System Requirements.....	5
Configuring Client Protection: Step by Step	6
Installing Outpost Office Firewall	6
Configuring Updates for Client Computers	6
Deploying Outpost Client Firewall on Client Computers	7
Configuring Protection Settings for Client Computers	7
Applying Settings to Client Computers	7
Installing Outpost Office Firewall	9
Configuring Agnitum Updates for Client Computers	9
Enabling Updates	10
Scheduling Updates	10
Configuring Connection Options.....	11
Monitoring Update Statistics	12
Deploying Outpost Client Firewall on Client Computers	12
Opening the GPO to Edit	13
Using Software Installation Policy to Install Outpost Client Firewall	14
Linking a GPO.....	15
Configuring Protection Settings for Client Computers	16
General Settings.....	17
Application Rules	17
Process Control.....	21
Global Rules	22
ICMP Settings.....	22
LAN Settings	23
Plug-Ins.....	24
Log Cleanup.....	25
Password.....	25
License.....	26
Advanced	27
Applying Settings to Client Computers	29
Monitoring Publication Statistics.....	29

Introduction

These days, as Internet dangers and risks increase exponentially, administrators of corporate networks are obliged to pay special attention to user workstation protection. Corporate servers can be very well protected, yet their client workstations may have backdoors for outside intrusions, which can be used to steal internal data or introduce confusion.

To reduce the amount of network traffic and to control Internet usage by staff, administrators are filtering web site content and blocking net advertisements.

Relying on users to protect their workstations is generally not advisable since most staff are not technically educated enough to build and maintain the strength of protection required to safeguard their computers that would prevent unauthorized access of the corporate network.

When the need arises to protect selected user workstations from intrusion and virus epidemics, the administrator usually has to visit each computer to manually install and configure its firewall to comply with corporate security policies. Practically always, the same settings and tools are used with each workstation. In complex distributed networks this requires an administrator to spend a lot of time duplicating the same sets of operations multiple times. Moreover, the administrator must manually reapply all modifications made by each individual user.

Additionally, each client itself has to download firewall updates that in large networks may result in excessive Internet traffic usage.

Until now, no firewall provided an easy mass installation and configuration of workstations across a network. Outpost Office Firewall, designed specifically to help administrators in protecting their networks from every attack vector, allows you to:

- Automatically install and configure client firewall which is based on Outpost Firewall Pro, the world's leading firewall software, on the client computers in your network to protect them from all known Internet threats using the proven and award winning Agnitum technologies.
- Modify each client's firewall configuration to comply with your corporate security policy. If users are permitted to perform configuration modifications, Outpost Office Firewall gives you the option to either overwrite their modifications or not.
- Control individual workstation protection from a central location (a server or dedicated workstation), create and automatically deploy protection configurations, as well as troubleshoot and monitor each firewall installation.
- Download one update and install it to all clients simultaneously to reduce the impact of this Internet traffic on your network bandwidth.

System Requirements

Components

In addition to the Outpost Client Firewall, Outpost Office Firewall contains the following management tools:

- Agnitum Command Center—the main managing tool that lets you control client firewall installations over your network and manage the other product components.
- Client Configuration Editor—the tool used to create and modify client firewall configurations.
- Agnitum Update Service—provides a centralized (single download, multi-install) client firewall update.
- Agnitum Publisher Service—provides for firewall configuration publication and transfer.

System Requirements

Outpost Office Firewall does not have to be installed on a server or domain controller. It can be installed on any dedicated workstation running Microsoft Windows 2000 or later.

Outpost Client Firewall can be installed on any computer running Windows 98/2000/XP or 2003 Server operating system.

Configuring Client Protection: Step by Step

Outpost Office Firewall's workstation protection configuration consists of the following steps to fully protect your network from all known Internet threats.

Installing Outpost Office Firewall

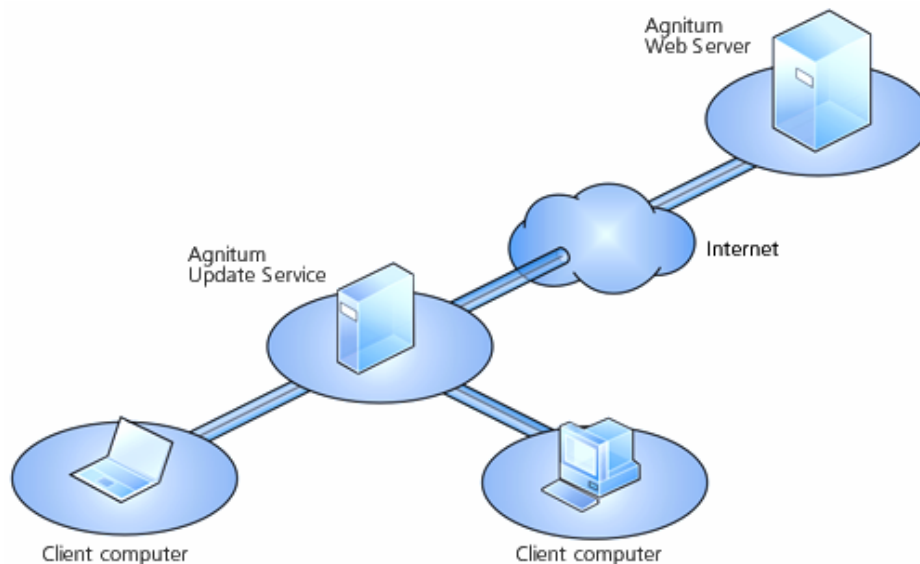
The first step is to install the administration management tools. Agnitum Command Center, the main managing application is implemented as an MMC snap-in. It lets you manage Outpost Client Firewall installations over the network and control the other Outpost Office Firewall components (Client Configuration Editor to create and configure firewall settings, Agnitum Update Service, and Agnitum Publisher Service to publish and transfer your firewall settings to clients). Outpost Office Firewall does not need to be installed on a server or domain controller. It can be installed on any dedicated workstation where the Agnitum Update Service and Agnitum Publisher Service are to be run. The computer where the Agnitum Command Center is installed is referred to as **the console**.

Note that Outpost Office Firewall itself does not install Outpost Client Firewall on the console. To protect the console, you can install the firewall during the second step described below or install it manually.

See the chapter [Installing Outpost Office Firewall](#) for details.

Configuring Updates for Client Computers

After the installation of Outpost Office Firewall is complete, you can configure the centralized automatic updates so when Outpost Client Firewall is installed on user workstations all available updates will be immediately applied so your network and each workstation always has the strongest and latest security. Centralized updates decrease network traffic. Agnitum Update Service provides automatic download and installation of each available update on all computers in your network. When configured it downloads all the necessary files from the Agnitum web site according to your specified schedule and makes them available to the clients on their request. When a client asks for an update, it is automatically downloaded from the console and installed, thus saving megabytes of Internet traffic.



Agnitum Update Service is configured through Agnitum Command Center.

See the chapter [Configuring Agnitum Updates on the Client Computers](#) for details.

Deploying Outpost Client Firewall on Client Computers

The next step is to deploy Outpost Client Firewall to the client computers in the Active Directory domain (Windows 2000 or later). This can be done via Group Policy using the **Software installation** policy. As the policy is applied to computers that are subject to the Group Policy Object (GPO) only, the GPO must be linked to the computers you want to protect, otherwise the policy will not be applied and Outpost Client Firewall will not be installed. You can then link the policy to any other computer and it will be applied during its next startup or unlink the policy from any computer (with or without uninstalling the firewall) if you decide to stop protecting that computer.

See the chapter [Deploying Outpost Client Firewall on the Client Computers](#) for details.

Configuring Protection Settings for Client Computers

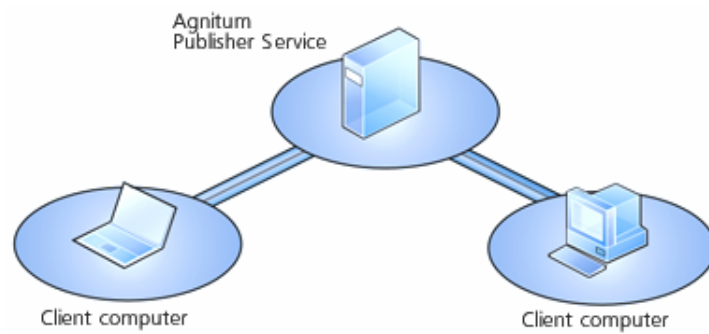
Once Outpost Client Firewall is installed on the user computers, you can configure their security settings. Client Configuration Editor is a special tool available with Outpost Office Firewall that lets you specify application and system rules, attack detection configurations and other firewall settings.

See the chapter [Configuring Protection Settings for the Client Computers](#) for details.

Applying Settings to Client Computers

After the desired settings are specified, they should be published, so the clients can pull the configuration changes when Outpost Client Firewall is installed on each computer.

This is done with the help of Agnitum Publisher Service, which can be configured using Agnitum Command Center. When a client computer pulls those configuration changes (every ten minutes), the new configuration is sent to that computer and applied without having to restart that client.



You can change the firewall configuration and republish it to the selected Outpost Client Firewall installations any time the need arises. For example, after installing a network application on user computers, you can create an on-the-fly rule and apply it to all the clients on your network.

See the chapter [Applying Settings to the Client Computers](#) for details.

Installing Outpost Office Firewall

To start installing Outpost Office Firewall, run the **setup.exe** 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: Agnitum Command Center, Client Configuration Editor, Agnitum Update Service, and Agnitum Publisher Service.

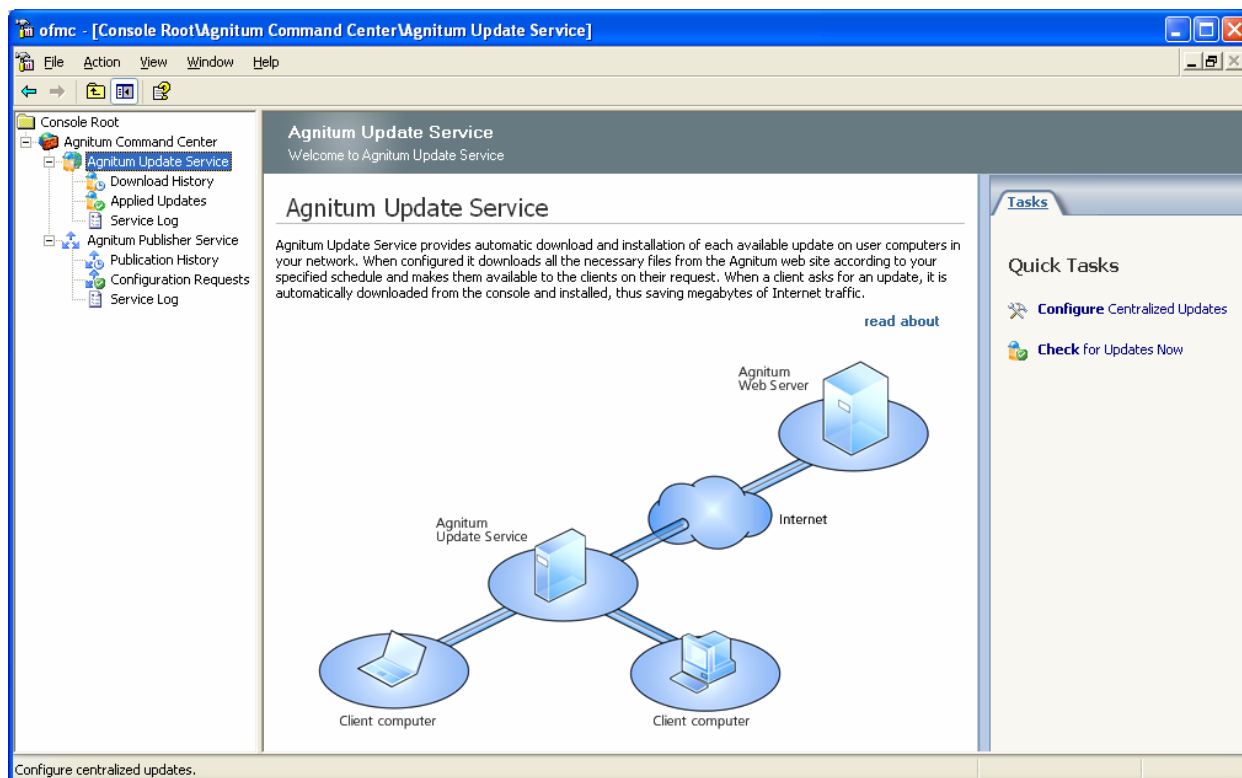
Note: If you need to install Agnitum Command Center and services on different servers, please see the [Technical Reference](#) for details.

During installation, the Outpost Client Firewall installation package will be copied to the folder **C:\Program Files\Agnitum\Outpost Office Firewall\Command Center\oofclnt**, which is automatically shared, so the installer is available to all clients on the network. Note that the installation wizard of Outpost Office Firewall does not install Outpost Client Firewall itself. If you want to protect the console, you can install the firewall during the second step described below or install it manually.

Important: Administrative rights over the console computer are required for working with Command Center. Make sure you have sufficient privileges.

Configuring Agnitum Updates for Client Computers

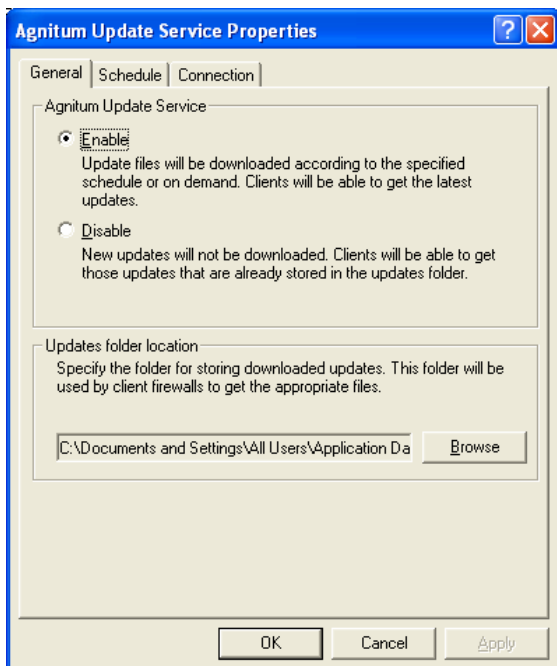
Modifying the update configuration is done through Agnitum Command Center. From the **Start** menu select **Programs > Agnitum > Command Center** to open the Agnitum Command Center MMC snap-in. Select **Agnitum Management Console > Agnitum Updates** and click **Configure Centralized Updates** in the quick tasks pane to open the update settings.



Enabling Updates

To enable updates, select the **Enable** option on the **General** tab of the **Agnitum Update Service Properties** window. When the updates are enabled, they are automatically downloaded hourly (unless the client is in **Block All** mode), according to the specified schedule, or on demand, transferred to each client on their request and applied. If you disable updates, new updates will not be downloaded and clients will be able to get the already downloaded files only.

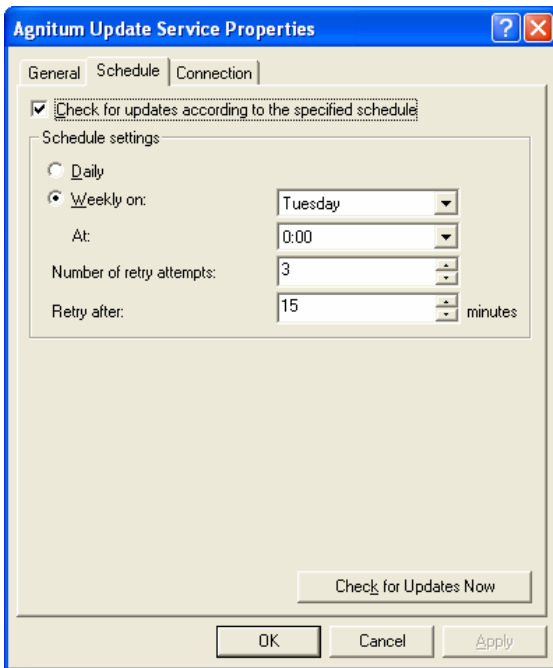
Note: Update files can be transmitted to clients only after the files are completely downloaded.



You can also specify the folder for storing downloaded updates.

Scheduling Updates

To schedule updates to be downloaded at a specific time, select the **Schedule** tab and be sure the **Check for updates according to the specified schedule** check box is selected. You can schedule daily or weekly updates and specify the number of connection attempts that Agnitum Update Service should make and the interval between attempts. An attempt is considered successful if an update is fully downloaded.



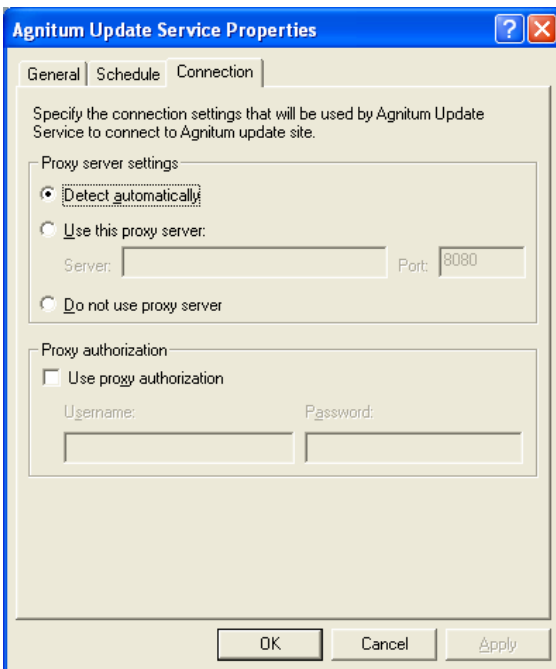
You can also check for updates immediately by clicking the **Check for Updates Now** button.

Configuring Connection Options

To specify the connection options that will be used by Agnitum Update Service to connect to the Agnitum update server, select the **Connection** tab.

If you use a proxy server for Internet connections, select **Detect automatically** to autodetect the proxy server parameters or **Use the following proxy server** to explicitly specify the address and port. Otherwise, select **Do not use proxy server**.

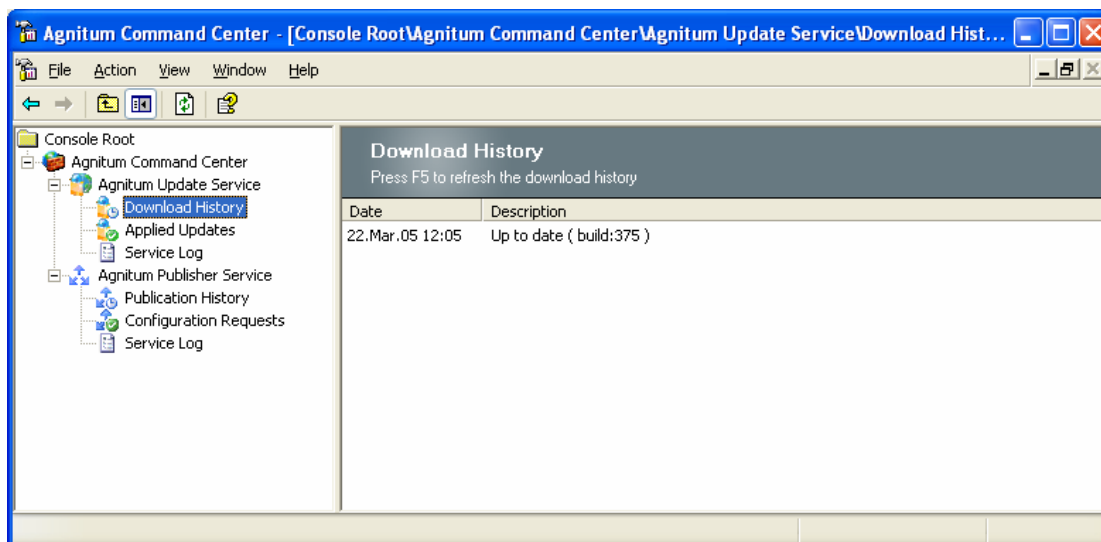
If a proxy server requires authorization, select the **Use proxy authorization** check box and specify the credentials.



Monitoring Update Statistics

Agnitum Command Center allows an administrator to control downloaded updates and whether or not they are to be applied to the required computers.

Select **Download History** in the left pane and in the right pane all the downloaded updates will be listed with the download date and description. The **Applied Updates** node lists the updates that were applied to specific computers. The **Service Log** node logs the service events.



Note: Please note that updates are transferred and applied to a client computer only by its request. If a client's firewall is disabled (not to be confused with the policy, **Disable Mode**), it cannot be updated until the firewall is enabled.

Deploying Outpost Client Firewall on Client Computers

For a small number of computers, you can install Outpost Client Firewall on each user's workstation manually (the client firewall setup package file, **agnitum outpost client firewall.msi**, is located in the folder **C:\Program Files\Agnitum\Outpost Office Firewall\Command Center\oofcInt**, which is shared during installation; see the **Outpost Client Firewall Maintenance Guide** for details). For many computers, you can automate this process for mass client firewall deployment. Once the client firewall setup is available on the network, the **Software installation** policy can be used to assign the setup package to each computer. To do this:

1. Open a GPO to edit.
2. Use the **Software installation** policy to install the client firewall.
3. Link the GPO.

Each step is explained in detail in the following sections.

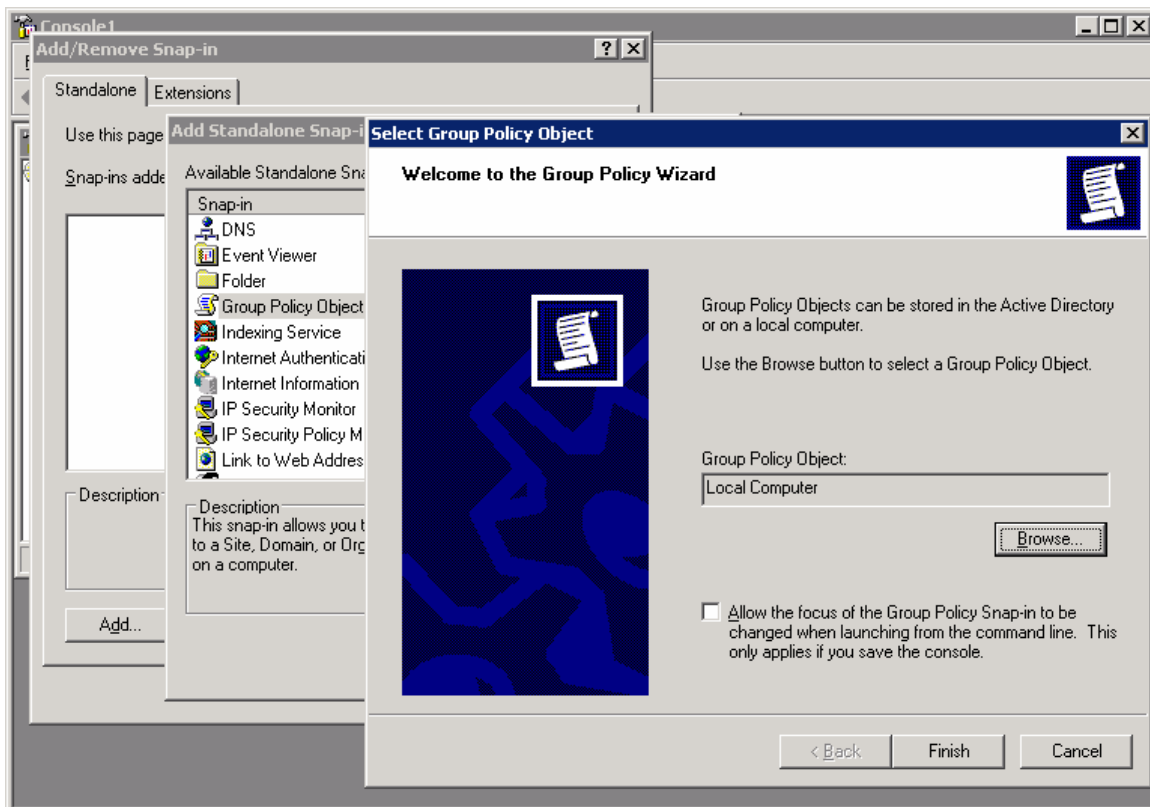
Note: Make sure to manually uninstall all previous Outpost Firewall versions from those computers you are going to protect. In this case the firewall configurations for those computers are not automatically supported. Also be sure to uninstall any other firewall software and reboot

before installing Outpost Client Firewall to prevent a system conflict of different firewalls fighting to control network access.

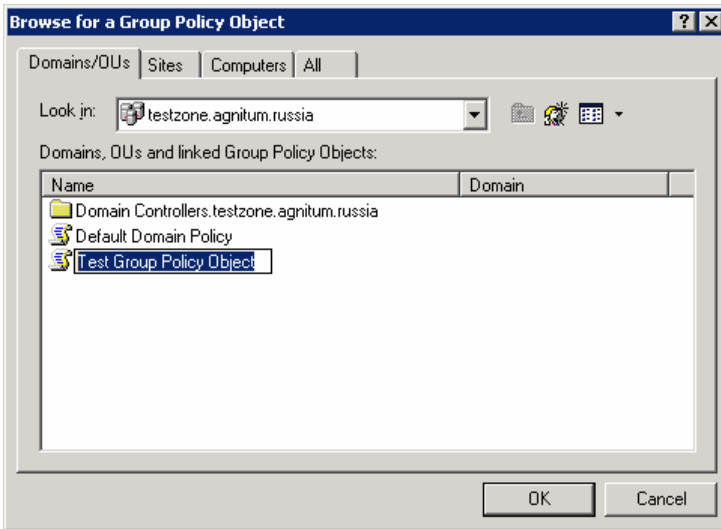
Note: See the [Technical Reference](#) for information on how to deploy Outpost Office Firewall in Windows NT domains and for pre-Windows 2000 clients.

Opening the GPO to Edit

Run MMC Console (**Start > Run > MMC > OK**) and add the *Group Policy Editor* snap-in: select **File > Add/Remove Snap-In**, click **Add** and select the Group Policy Object from the list. Click **Add** and you will be prompted for the GPO to edit.



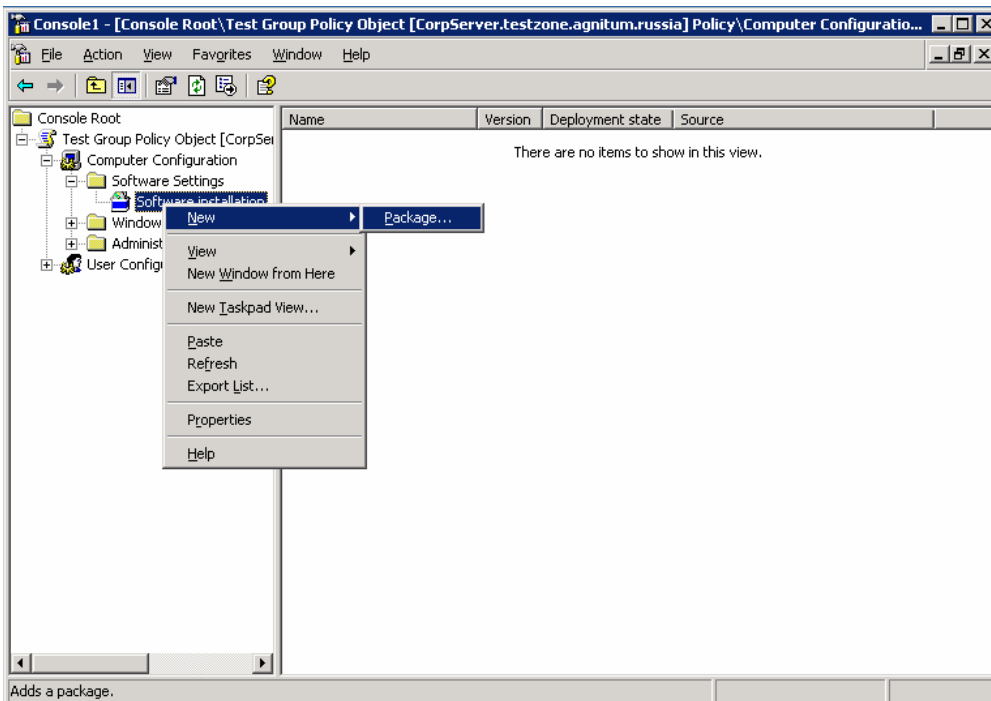
Click **Browse** to select the GPO. You can create a new GPO by clicking on **Create New Group Policy Object** or selecting an existing one (*Default Domain Policy*, for example).



Click **OK** when you are done. Click **Finish** and then **Close** to close the windows. After you click **OK**, the Group Policy Object Editor starts so you can edit the selected GPO.

Using Software Installation Policy to Install Outpost Client Firewall

Once the installation folder is created and shared during the installation of Outpost Office Firewall, the client firewall setup package is available on the network. You then need to set up the **Software installation** policy to assign the client firewall setup to user computers. Right-click the **Software installation** node in **Computer Configuration > Software Settings** and select **New > Package**.

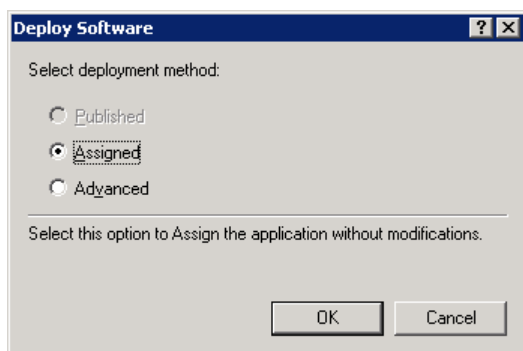


Browse to the installation folder (\\<ConsoleName>\oofcInt by default) and select the client firewall setup package.

Notes: Specify a UNC path to the installation package. For example, \\server\ oofcInt.

If the installation folder is located on an NTFS volume, you should set the appropriate NTFS permissions on the installation folder manually to make the folder available to clients. Also, make certain the clients have *Read* permission on the client firewall installation package.

In the **Deploy Software** dialog box, select **Assigned** and click **OK**.

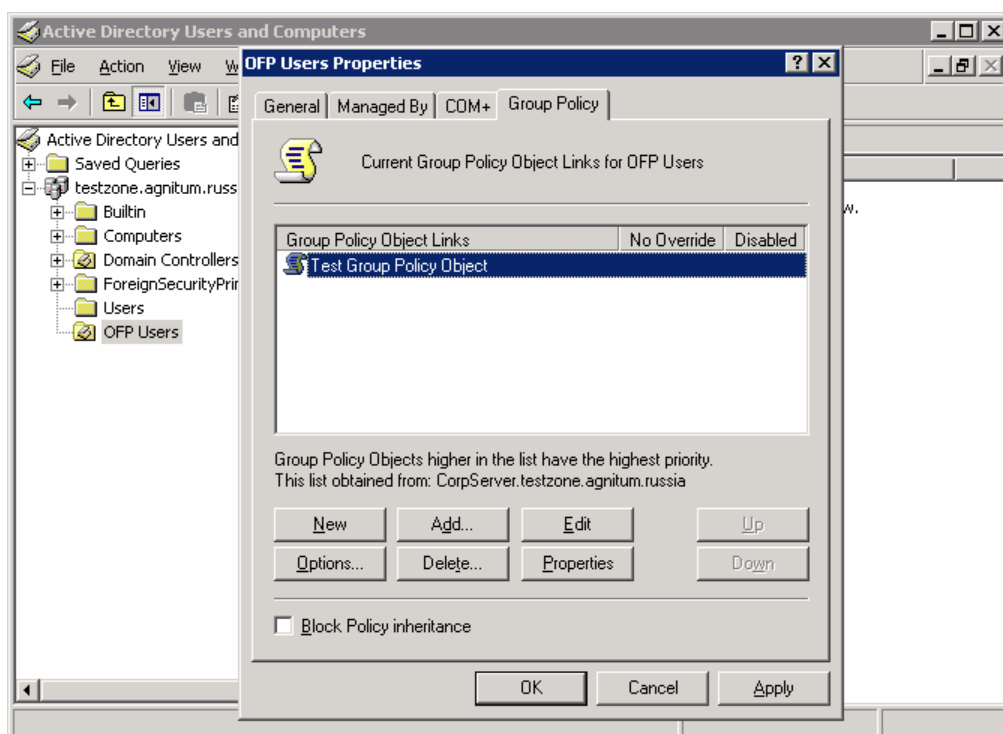


You will see a software installation policy record for the selected package in the right pane of the MMC console window. The client firewall setup will be installed the next time each client computer starts up regardless of which user logs onto it if the GPO is linked to the computer.

Note: See the documentation on administering group policies for detailed information on deploying software applications using a group policy.

Linking a GPO

Linking the GPO is performed from the *Active Directory Users and Computers* snap-in if the link is to domains or organizational units (OUs), or from the *Active Directory Sites and Services* snap-in if the link is to sites. Right-click the site, domain, or OU to which the GPO should be linked and click **Properties**. On the **Group Policy** tab click **Add** and select the desired GPO. After clicking **OK** twice, the GPO is linked to the object.



Notes: See the documentation on administering group policy for detailed information on linking GPOs and filtering the GPO scope to the required users and groups.

You can also use the *Group Policy Management Console* for linking the policy.

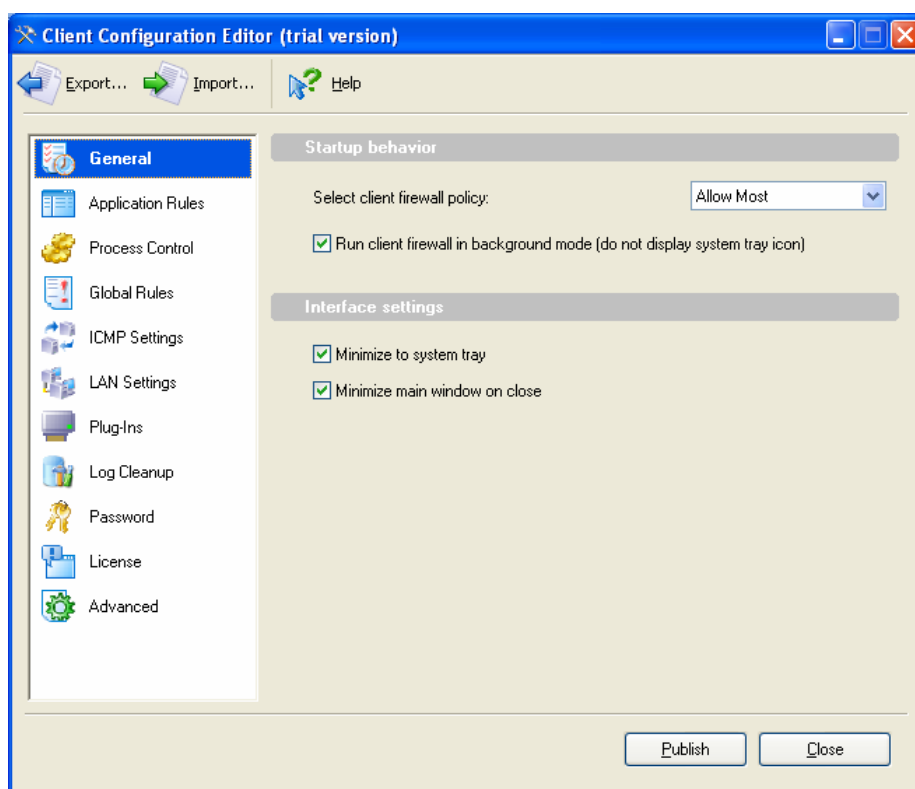
To be able to link GPOs to objects, the *Manage Group Policy Links* right on the site, domain, or organizational unit should be delegated to the account you are logged in under.

A client firewall can also be deployed using logon scripts. For details of how this is done, see the [Technical Reference](#).

Configuring Protection Settings for Client Computers

Firewall settings on client computers are configured using the special tool, Client Configuration Editor. In Agnitum Command Center, select the **Agnitum Publisher Service** node and click **Configure Clients** in the right pane.

This tool has all the Outpost Client Firewall settings, so the configuration process is convenient and easy to use for those administrators who are already familiar with earlier Outpost Firewall versions.



After the settings are specified, you can immediately publish the newly created configuration for all computers by clicking the **Publish** button.

Outpost Client Firewall has very many settings. A configuration is the state Outpost Client Firewall is in at any time. Being able to save several different configurations of these settings lets you:

- Create different configurations for your clients
- Switch between these configurations
- Back up configurations.

You can create several different configuration files simply by giving each a different name. To save the created configuration, click **Export** and enter the name you want to give that configuration.

To change clients to an earlier prepared configuration, use the **Import** button and choose the configuration file you want.

All the settings that are available for remote configuration are discussed below. You can find more detailed description of each setting in the **Outpost Client Firewall User Guide**.

General Settings

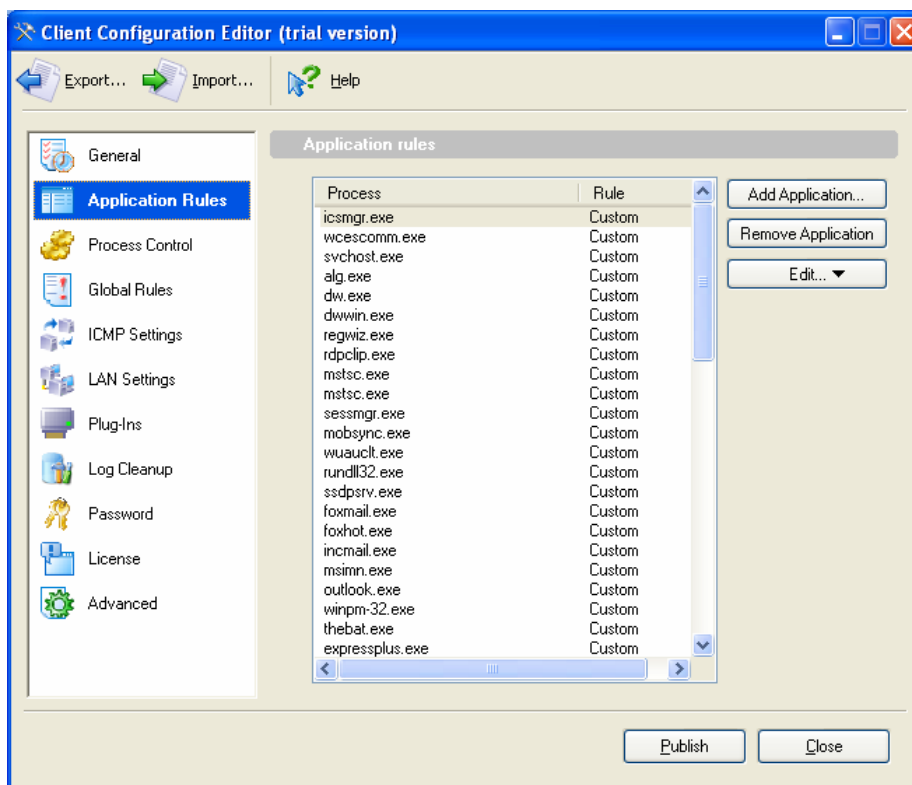
This tab allows you to select a policy for client firewalls to use and the mode they are to run in. By default, a firewall runs in background mode to eliminate user interference, save system resources, and for a systems administrator to block unwanted traffic or content in a way that's completely hidden from a user. The default policy is **Allow most**.

If some of a user's custom applications that require network access are blocked and you consider the user experienced enough to manage all the network access request messages, you can turn the background mode off and enable **Rules Wizard** mode on that computer.

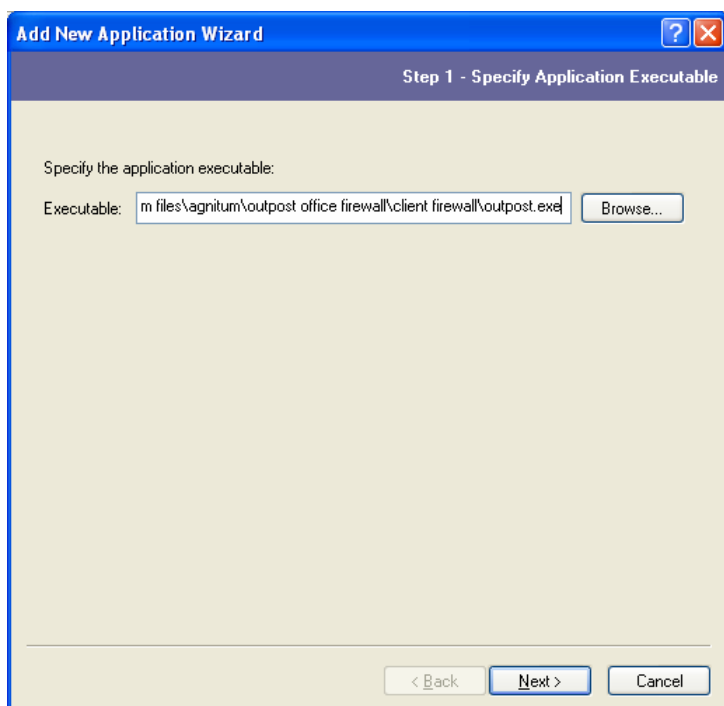
You can also set whether the firewall's main window should be minimized to the system tray on close.

Application Rules

The **Application Rules** page lets you define which applications on the user computer should have access to the network and which should not.

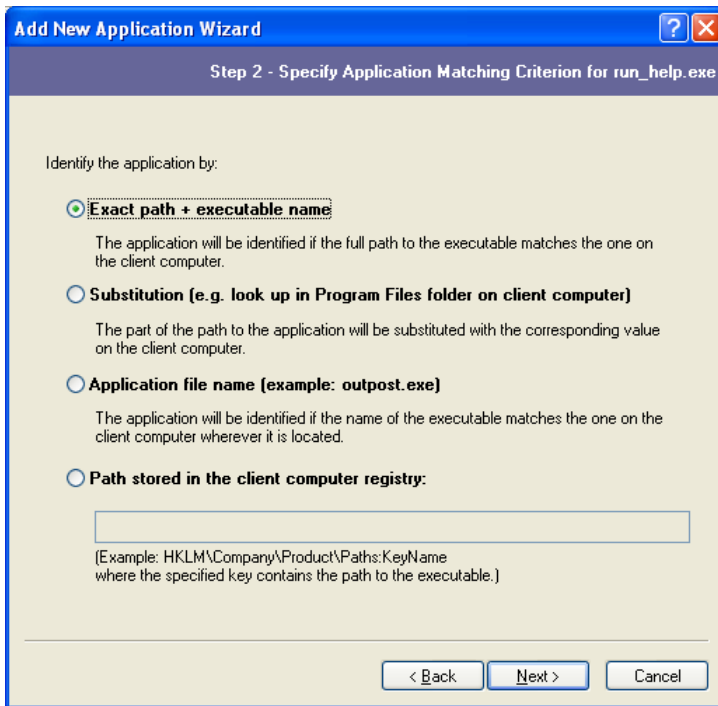


Click **Add Application** to create a set of rules for a new application. The **Add New Application Wizard** will ask you for the application executable file. Specify the file and click **Next**.



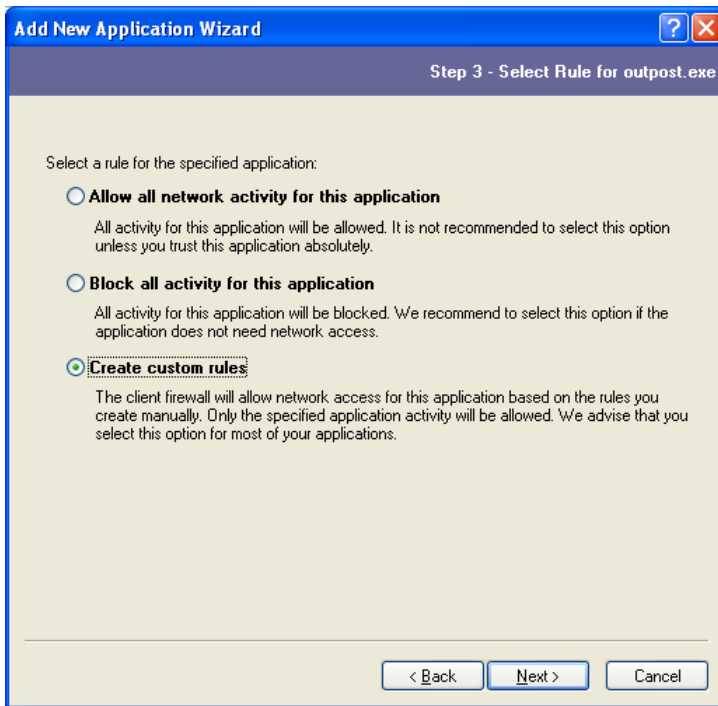
The next step lets you specify a matching criterion for identifying the application on the client computer. You can select one of the following criteria:

- **Exact path + executable name**—to identify the application by the full path to its executable.
- **Substitution**—if the application is installed in one of the well-known folders (such as **Program Files** or **Windows\System32**, for example), the path to this folder on the console will be substituted with the path to the corresponding folder on the client computer.
- **Application file name**—the application will be identified by its file name wherever it is installed on the client computer.
- **Path stored in the client computer registry**—the path to the application will be taken from the specified registry key on the client computer. If you leave the text box clear, the application file name will be searched in the **HKLM\Software\Microsoft\Windows\CurrentVersion\App Paths** registry key.

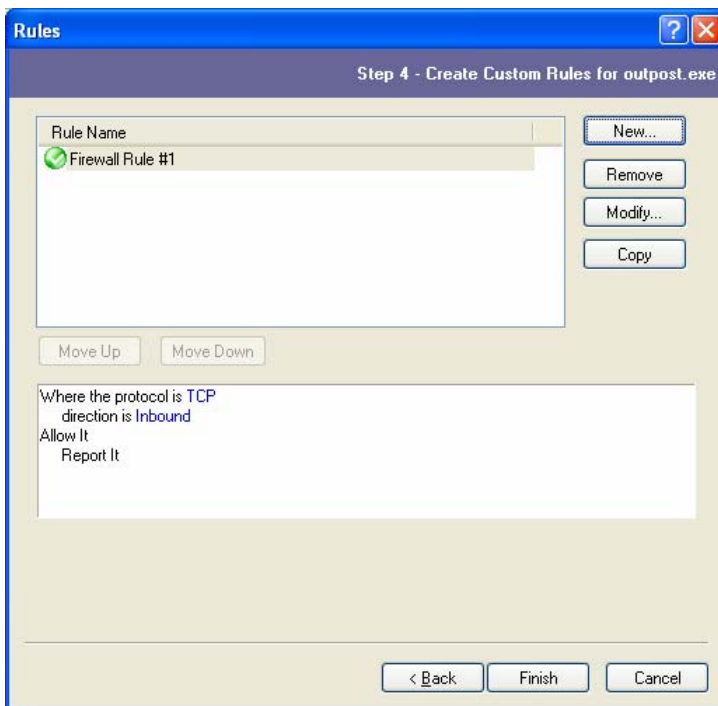


After clicking **Next**, you will be prompted for the rule according to which the application will be granted network access on the client computer. You can either:

- **Allow all network activity for this application**—all activity for this application will be allowed. This option is not recommended unless you trust the application absolutely.
- **Block all activity for this application**—all activity of the application will be blocked. We recommend that you block all applications that do not need Internet access, such as text editors, calculators, etc.
- **Create custom rules**—Outpost Client Firewall will allow access to the Internet for the application based on the rules that you will create manually. Only the specified application activity will be allowed. We advise that you create rules for most of your applications.



If you select to create rules, the next step will let you specify rules for the added application.



Rules editing is performed the same way as in Outpost Client Firewall. See the **Outpost Client Firewall User Guide** for details on creating application rules.

Click **Finish** to exit the wizard and you will see the new application in the list.

Client Configuration Editor suggests the default preset rules for the most popular applications, which you can change by creating additional rules for the client applications or editing/deleting the existing ones. Click **Edit > Modify Rules** to change the rules and matching criterion for the selected application. Also, use the **Edit** button menu to toggle between the **Trusted/Blocked/Custom** application categories.

After the configuration is applied to the client, the applications specified on this page will be matched with those on the client computer using the specified matching criteria, and the rules for the matched applications will become active.

Note: The rules from the published configuration are merged with the existing rules on the client computer.

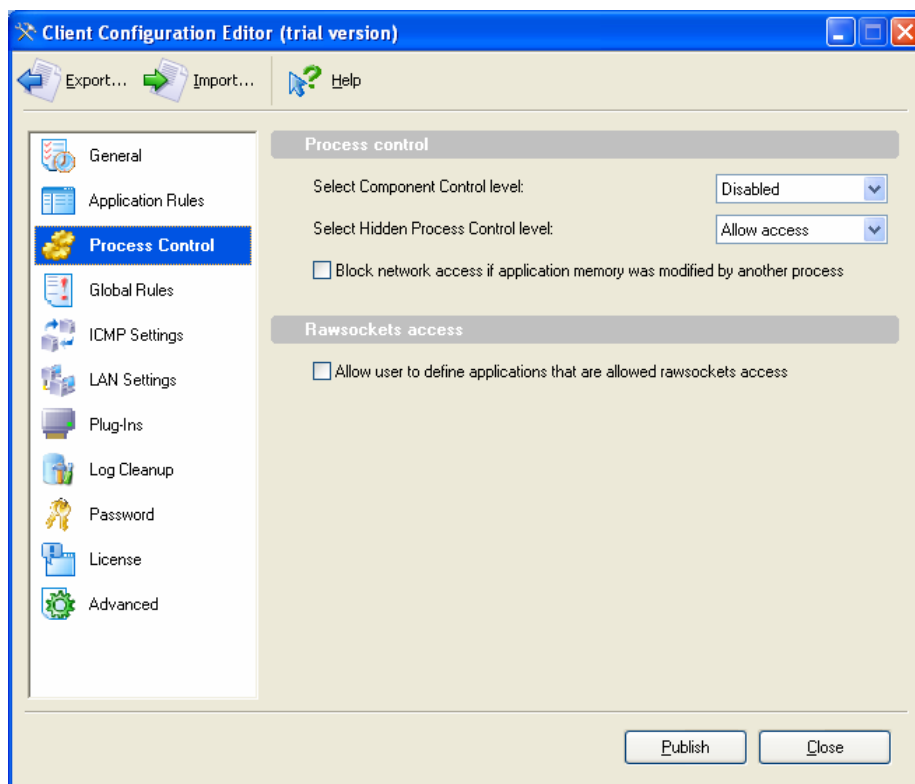
Process Control

The **Process Control** settings allow you to enable additional Outpost security technologies such as Component Control, Hidden Process Control and Open Process Control. This protection is disabled by default, but if you consider your users experienced enough to manage the enormous number of network access request messages, you can enable it.

Component Control monitors the components of each application to make sure they are not fake or malicious. You can set the desired Component Control level using the corresponding drop-down list.

Hidden Process Control lets you control processes that are ran on behalf of a trusted application so these cannot perform inappropriate activities. You can select the desired policy for hidden processes using the corresponding drop-down list.

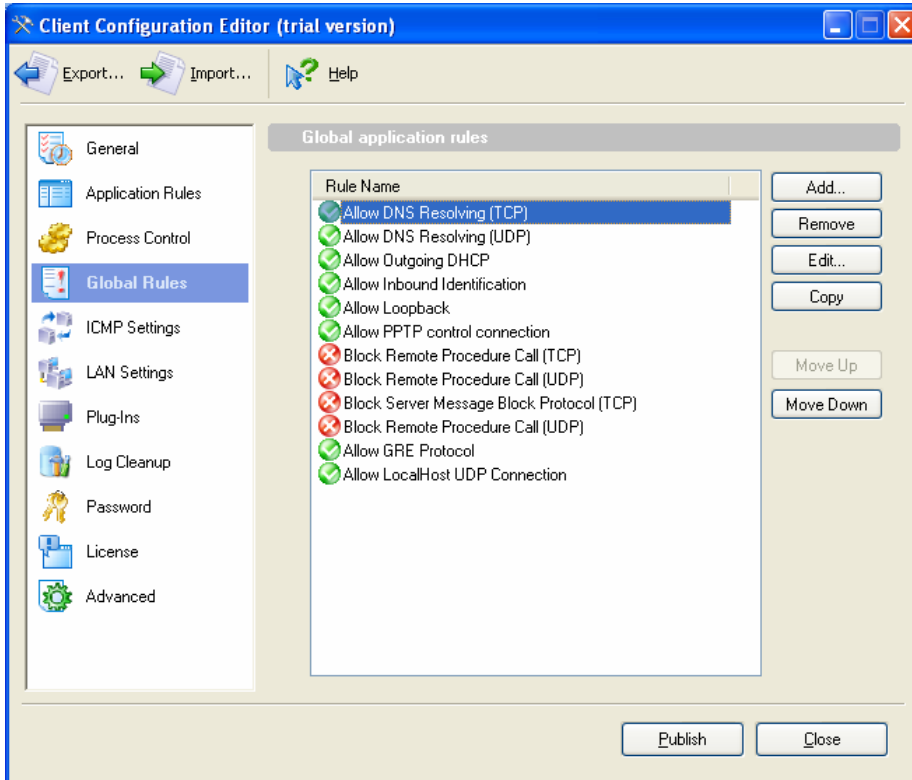
Open Process Control lets you control those functions that can be used to inject malicious code into a trusted application's address space and so prevents rogue processes from modifying process memory. Select the **Block network access if application memory was modified by another process** check box to enable this protection technique.



Also, you can allow user to define which applications are allowed to make rawsocket calls (direct low-level socket calls) by selecting the corresponding check box.

Global Rules

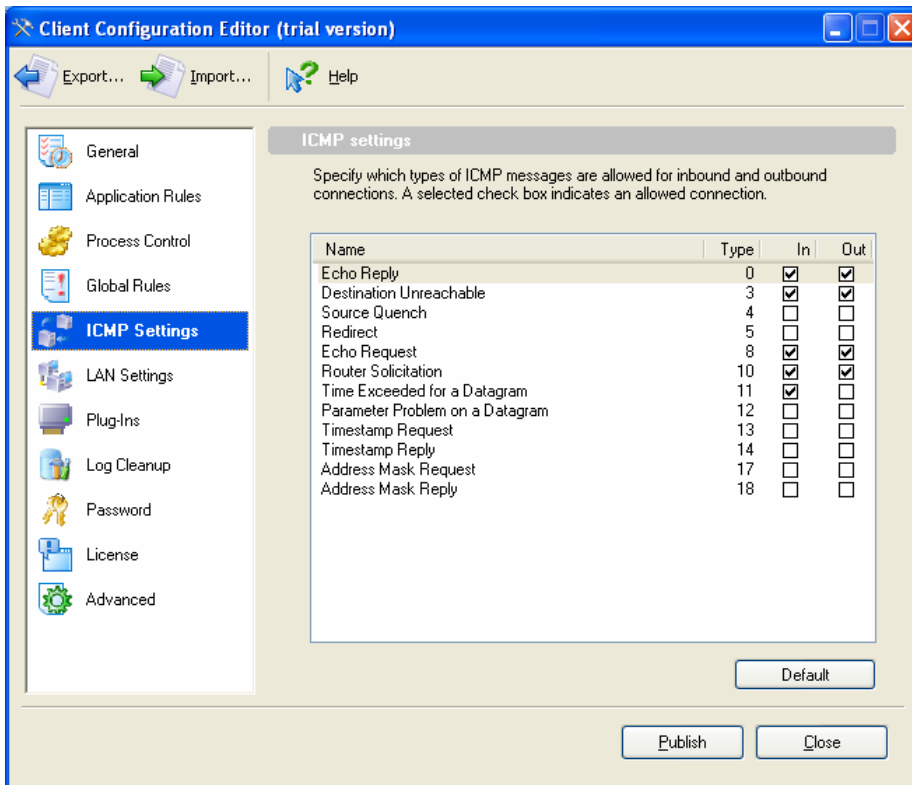
The **Global Rules** tab lets you specify global application rules that are of high priority for all applications. Click **Add** to create a new rule and **Edit** to edit an existing one. The rules are applied top-down. See the **Outpost Client Firewall User Guide** for details on editing global rules.



Note: The rules from the published configuration are merged with the existing rules on the client computer.

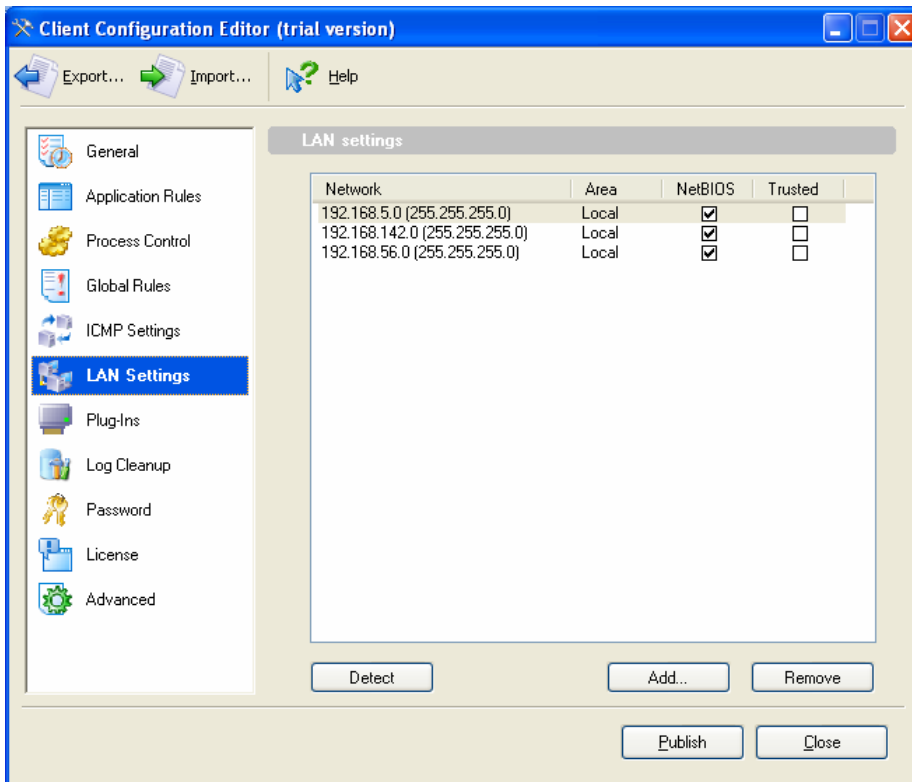
ICMP Settings

These settings let you specify the types of inbound and outbound ICMP messages to be allowed. To allow a connection, select its check box. Click **Default** to revert to the out-of-the-box settings.

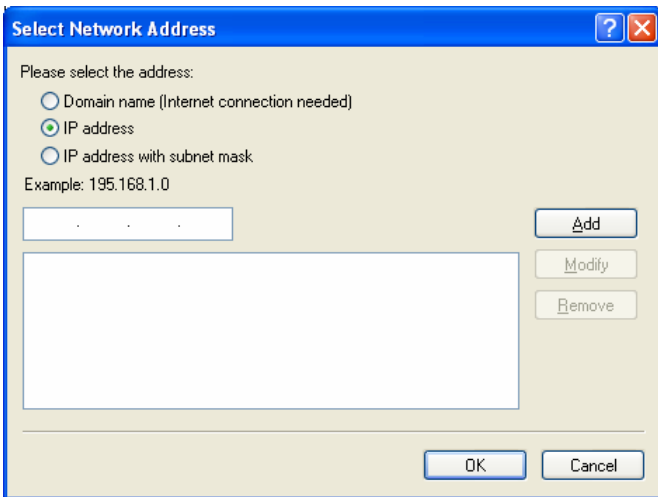


LAN Settings

This tab lets you change the settings for the local area network, which a user's computer belongs to, his NetBIOS choices, and lets you add or remove trusted IP ranges.



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.

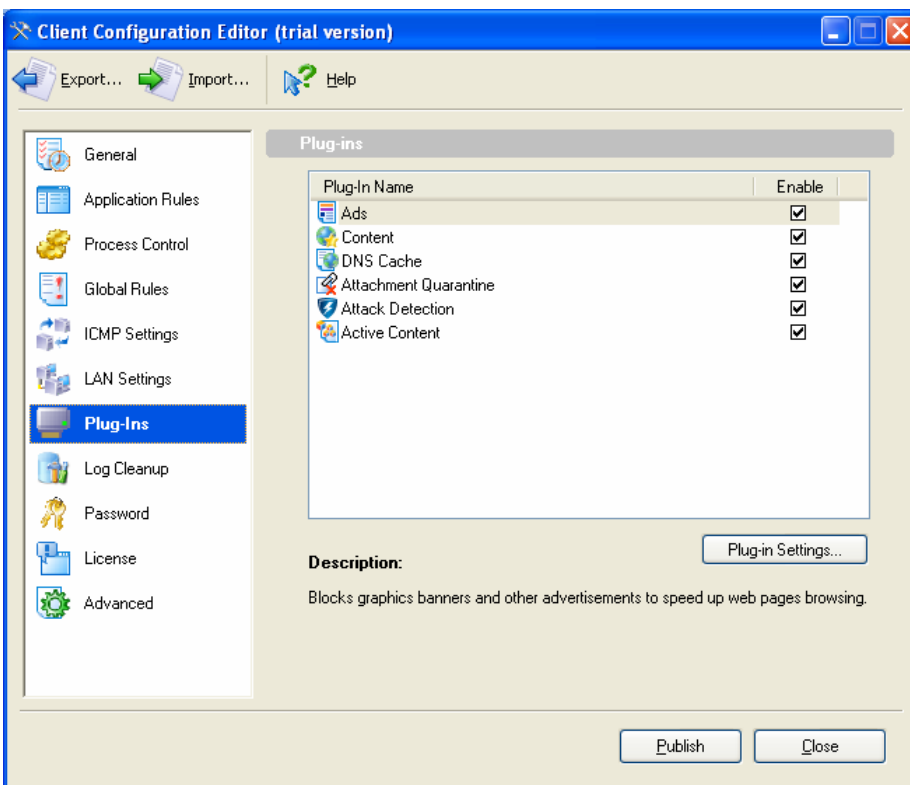


If you wish to allow all connections for a particular network, add the network address to the list and select the corresponding check box in the **Trusted** column. Otherwise, if you want to remove a network address from the **Trusted Zone**, clear its check box.

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

Plug-Ins

This tab allows you to configure Outpost Client Firewall plug-ins on client computers. Select the plug-in which settings you want to alter and click **Plug-In Settings**. The settings dialog boxes are just the same as in Outpost Client Firewall itself.

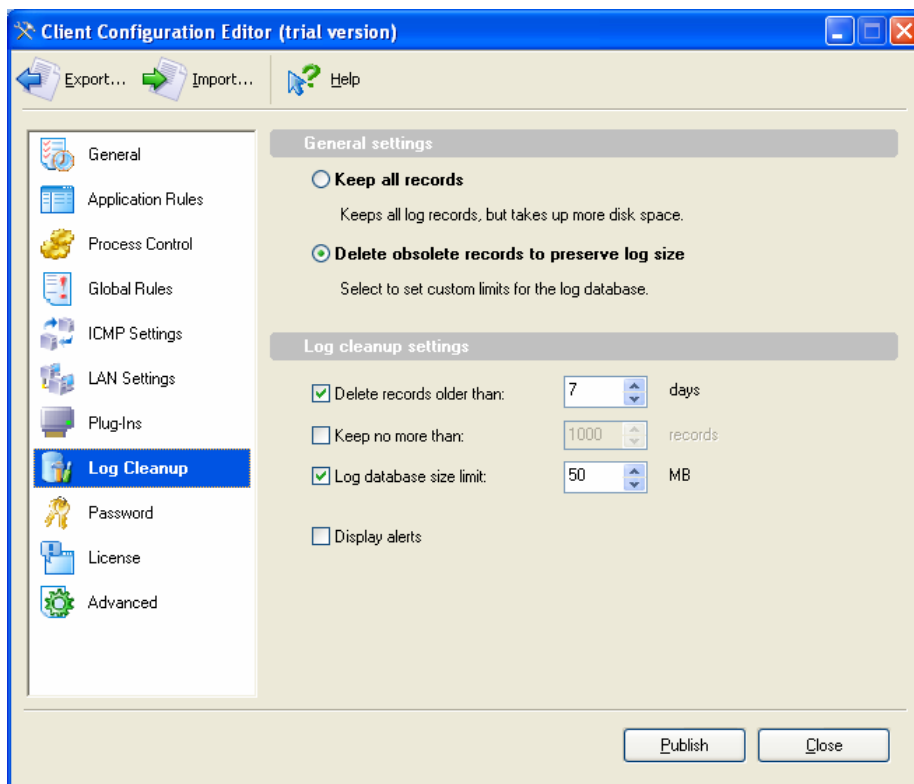


Log Cleanup

To specify the Outpost Client Firewall log cleanup settings on client computers, select the **Log Cleanup** tab. Select **Delete obsolete events to preserve log size** to have the Log Cleaner automatically remove outdated log entries from the database or select **Keep all records** to disable the Log Cleaner.

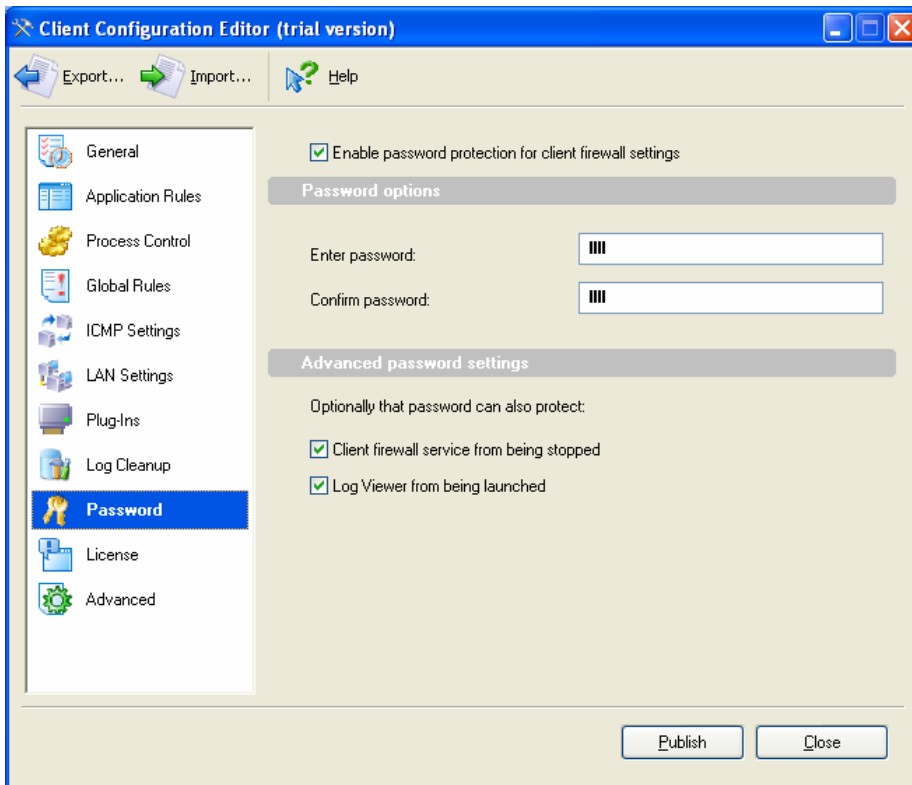
Specify the age in days after which events are considered outdated, the maximum number of the most recent event records to keep in the log and the **Log database size limit**, a value in megabytes, that determines how large the log database should be allowed to grow.

Select **Display alerts** to have the Log Cleaner display all notification messages to the user during the cleanup process.



Password

You can specify a password, to protect the Outpost Client Firewall settings on client computers from being changed by users. Click the **Password** tab, select **Enable password protection for client firewall settings**, and specify the password in the text box provided. Confirm the password and specify whether it should also protect the Outpost Client Firewall service from unauthorized stopping and the Log Viewer from being launched.

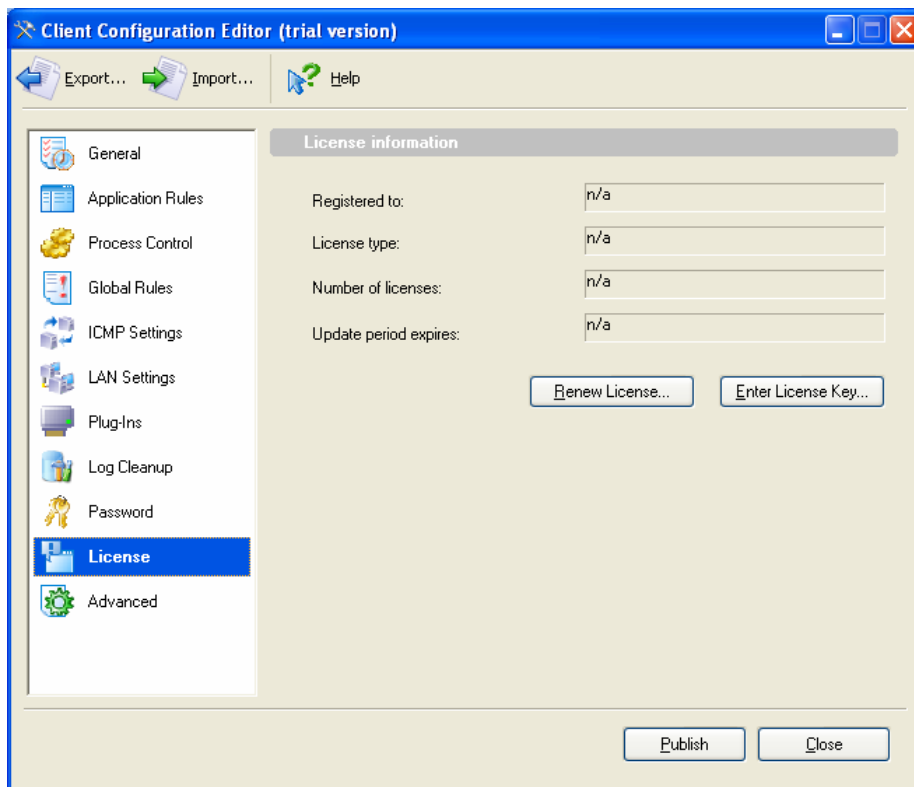


For information on how to protect only specific firewall settings from being modified, see the [Settings Priority](#) section below.

License

This tab displays your current license information. If you want to renew your license, click on **Renew License** and you will be redirected to the appropriate page on the Agnitum web site.

You can also enter your license key by clicking on **Enter License Key** to register all your client firewalls. The license key will be sent to each client when it requests the configuration files provided by the Agnitum Publisher Service.



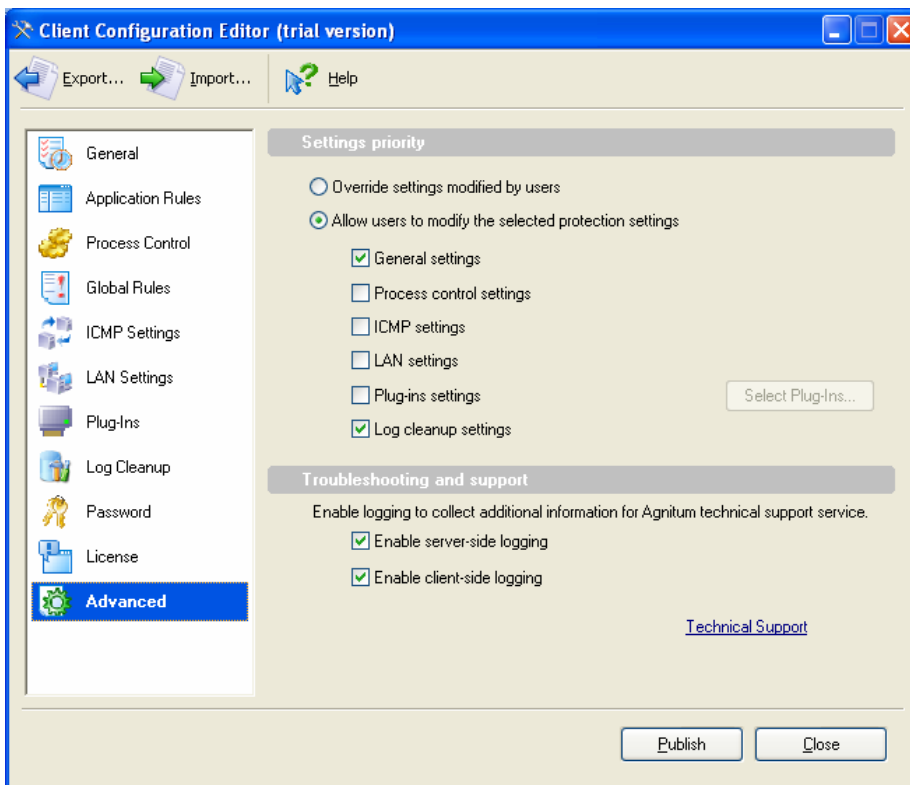
Advanced

The last tab lets you define whether users are allowed to make changes to the firewall settings or if all the settings should be taken by clients from the console and cannot be altered.

Select **Override settings modified by users** if you do not want to allow users to modify the firewall settings. In this case, even if a password is not set to protect firewall settings and the settings were modified, they will be overwritten the next time the published configuration is requested.

If you want to allow users to modify some settings, select the **Allow user to modify the selected protection settings** option and select the settings a user will be able to modify. These settings will not be overwritten while applying the requested configuration.

Note: You cannot prohibit users from modifying application and global rules, unless you set a password to protect firewall settings. The rules from the published configuration are always merged with the existing rules on a client computer.

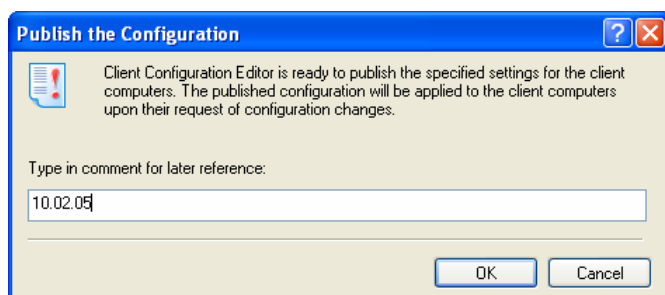


Additionally, you can enable client and server-side logging in case you have any issues regarding the product operation. The collected information can be provided to Agnitum support service and will be helpful in resolving your problems.

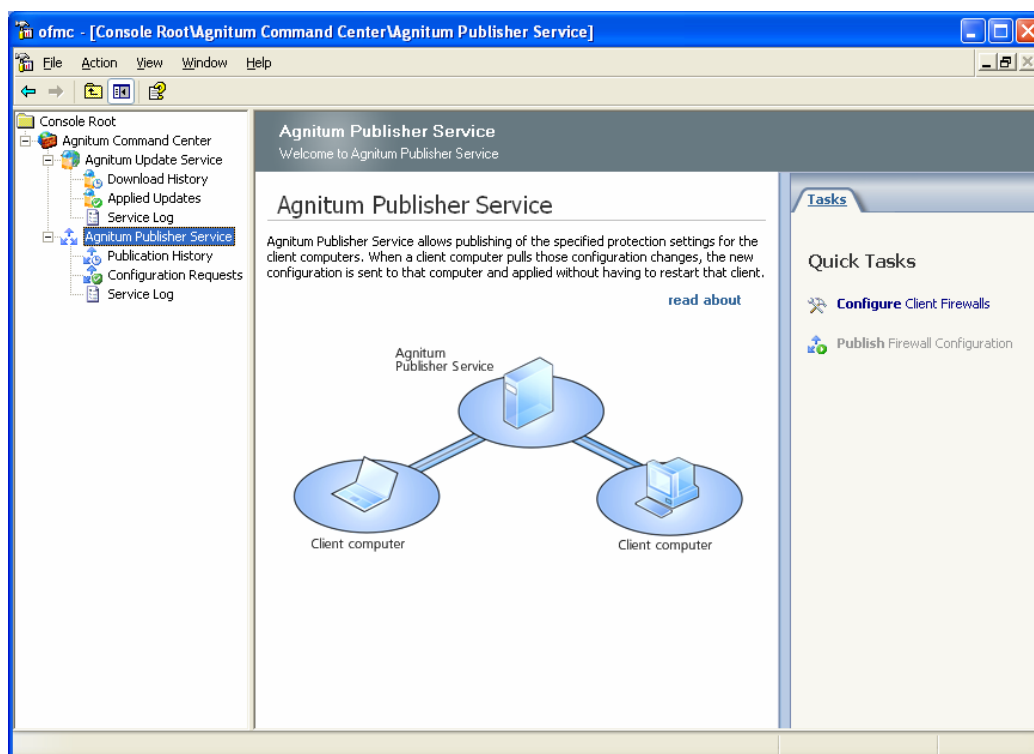
Applying Settings to Client Computers

After you have specified the desired settings for the firewall on client computers, the created configuration files need to be published so each client can retrieve and apply those settings. You can publish the configuration directly using the Client Configuration Editor by clicking **Publish** or do it later from the Agnitum Command Center.

Select the **Agnitum Publisher Service** node and click **Publish Configuration** in the quick tasks pane. You will be prompted for a comment to the configuration to be referenced by and after clicking **OK** the configuration will be available to the clients.



You can reapply another configuration later by simply copying the configuration file to the appropriate location and clicking **Publish Configuration**. The new settings will be transmitted to the client on its request and immediately applied without computer restart.

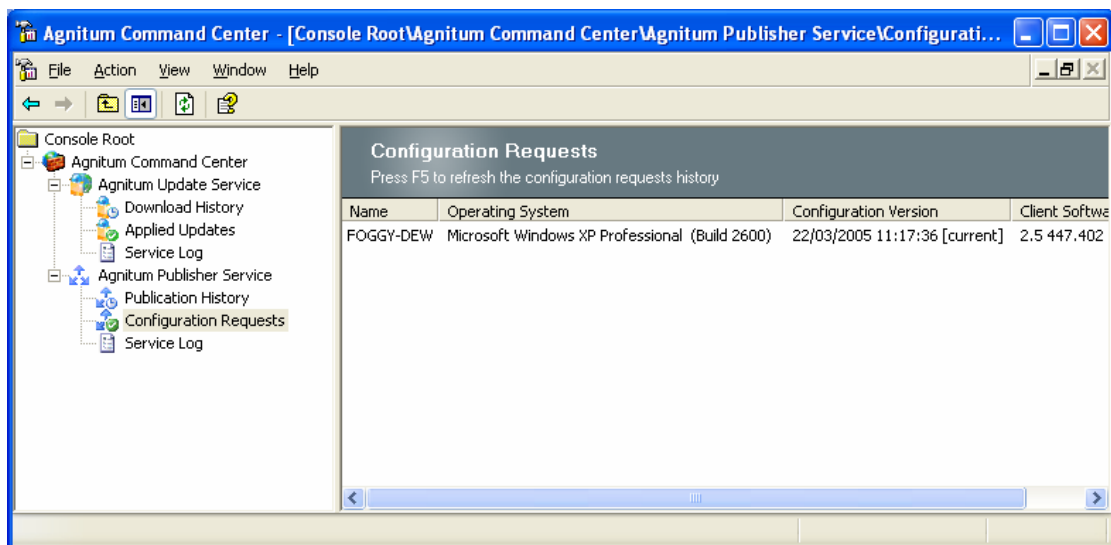


Monitoring Publication Statistics

Agnitum Command Center lets the administrator control published configurations and to find out whether or not they were applied to the designated computers.

Select the **Publish > Publication History** in the left pane and in the right pane all the configurations that were transferred to clients will be listed with the transfer date and

description. The **Configuration Requests** node displays the current configurations of individual computers. The **Service Log** node logs the service events.



Note: Please note that configurations are transferred and applied to client computers only on their request. If a client firewall is disabled (not to be confused with the **Disable Mode**), the client cannot get the configuration until its firewall is enabled again.