

Maintenance  
Guide

# Outpost Firewall 4.0

Personal Firewall Software  
from  
**Agnitum**

## Abstract

This document is intended to assist Outpost Firewall users in installing and maintaining Outpost Firewall and gets users acquainted with Outpost Firewall setup, Agnitum Update and Outpost Firewall Log system maintenance.

# Table Of Contents

- 1     INSTALLING OUTPOST FIREWALL..... 4**
- 2     UNINSTALLING OUTPOST FIREWALL..... 13**
- 3     KEEPING YOUR PROTECTION UP-TO-DATE ..... 14**
- 4     LOG DATABASE MAINTENANCE..... 17**
  - 4.1 DATABASE CLEANUP ..... 17
  - 4.2 REPAIRING THE LOG DATABASE ..... 18
- 5     TECHNICAL SUPPORT ..... 19**

# 1 Installing Outpost Firewall

**Outpost Firewall's** installation procedure is similar to that of most Windows programs.

**Notes:**

- Be sure to uninstall any other firewall software and **reboot** before installing **Outpost Firewall** to prevent a system conflict of different firewalls fighting to control network access.
- If you are installing **Outpost Firewall 4.0** over an older version, the setup program will ask you whether you want to retain your configuration settings.

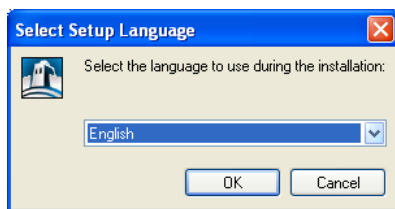
To start the installation program of the **Outpost Firewall** system:

1. **Very Important!** Before installing **Outpost Firewall**, uninstall any other firewall software on your computer and **reboot**.
2. Close all open applications.
3. Click the **Start** button on the Windows task bar.
4. Select **Run** on the **Start** menu.
5. In the **Open** field of the **Run** dialog window, enter the full path to the setup program file (OutpostProInstall.exe). For example, if the setup program is on disk **D:** in the folder **Downloads** and subfolder **Outpost**, type into this field:  

```
D:\downloads\outpost\OutpostProInstall.exe
```
6. Click the **OK** button.

The setup wizard contains several steps. Each step has a **Next** button that takes you to the next step of the procedure, a **Back** button that returns you to the previous step and a **Cancel** button that exits the wizard and aborts the entire setup procedure.

The installation begins with **Select Language** dialog.

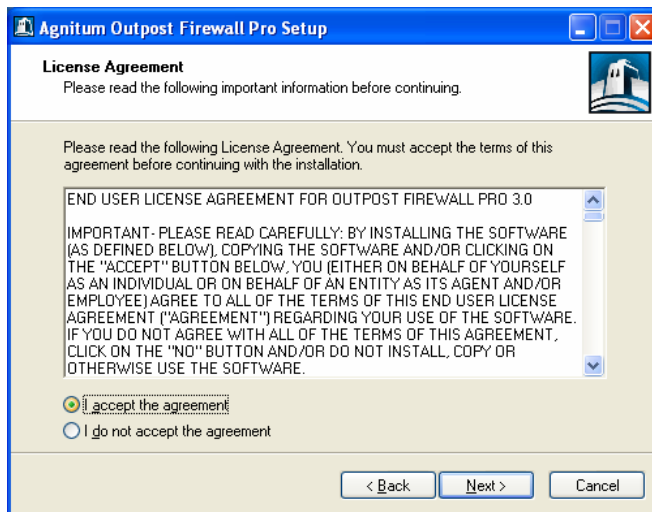


Choose the language for **Outpost Firewall** interface and click **OK**. Setup will display the **Welcome** dialog that reminds you to close all running applications.

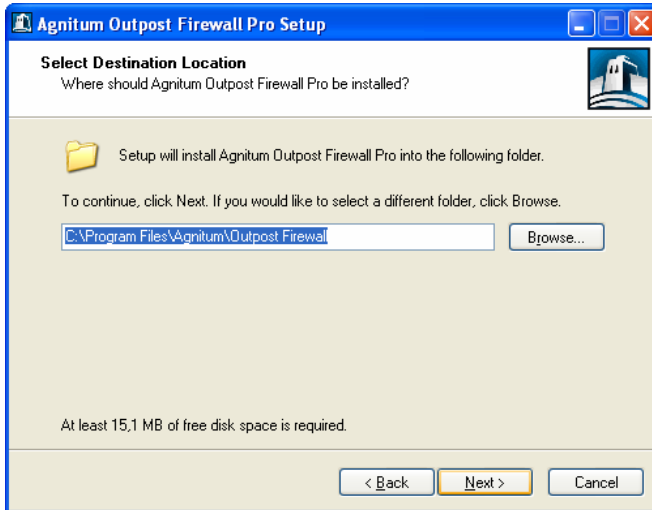


After clicking the **Next** button you will be asked to accept the License Agreement to use the **Outpost Firewall**.

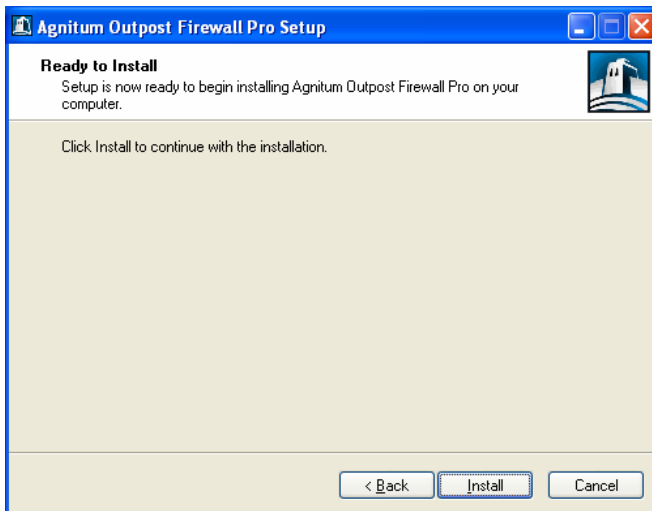
Please read it carefully. This dialog's **Next** button is enabled only if you select the option button **I accept the agreement** indicating that the License Agreement is acceptable to you.



After you have accepted the License Agreement, the **Next** button brings you to the **Select Destination Location** step:

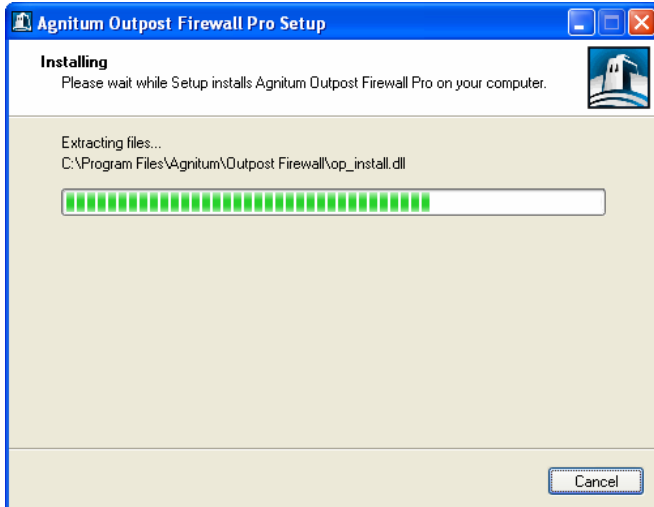


Click **Next** to proceed to the last step before actual installation:



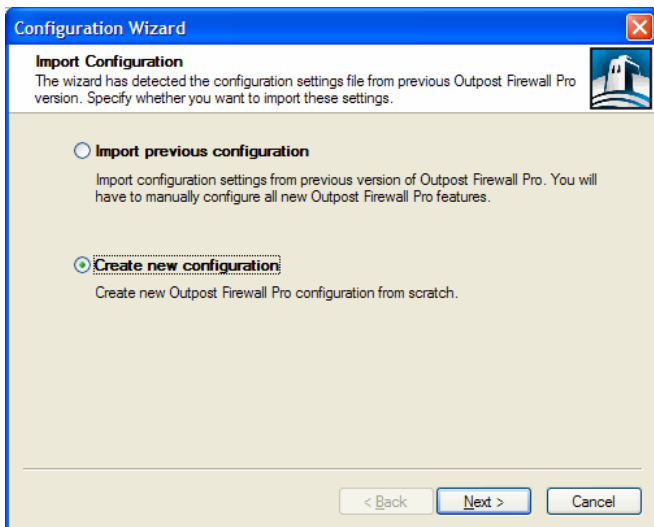
When you are ready to go ahead with the installation, click the **Install** button.

The program displays the installation progress window:

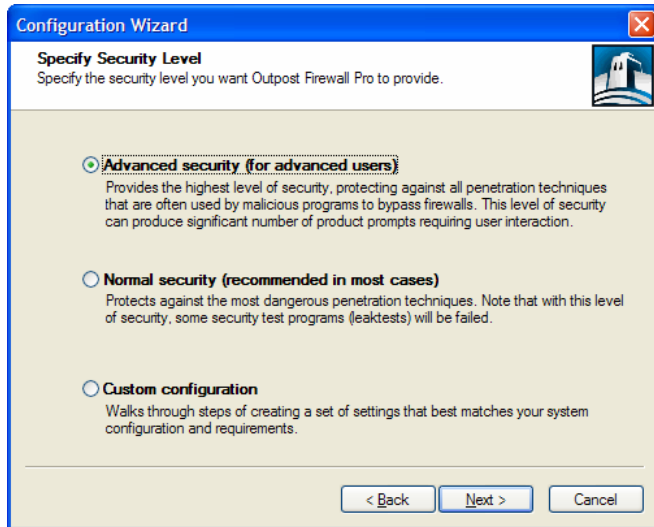


After the installation is finished, the **Configuration Wizard** will help you create a new configuration.

If you are installing over previous version, you can specify whether you want to preserve your configuration or create a new one from scratch.

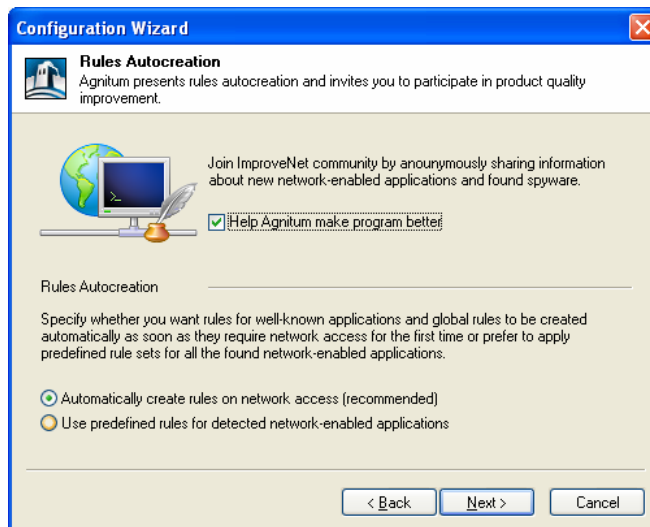


After selecting **Create new configuration** and clicking **Next**, Configuration Wizard provides two ways to configure your firewall: automatic configuration or by letting the Configuration Wizard help you. The next step lets you select whether you want to create a configuration automatically or specify each of its settings manually.



- **Automatic configuration.** You can select an automatic configuration that conforms to the security level you'd prefer. Two levels are available: **Advanced security** provides the best protection against all penetration techniques that are often used by malicious software to bypass firewall software and **Normal security** ensures protection only against the more dangerous techniques (for details, see the **3.7 Anti-Leak Control** chapter in Outpost Firewall Pro User Guide). **Normal security** has a reduced number of product prompts that require your response and is recommended for most cases.

Automatic configuration is much faster than custom. After you select either **Advanced security** or **Normal security** and click **Next**, the **Rules Autocreation** step is displayed, which allows you to enable rules autocreation, so that global rules and rules for well-known applications are created automatically when they first request an action (for example, network access or process memory modification).



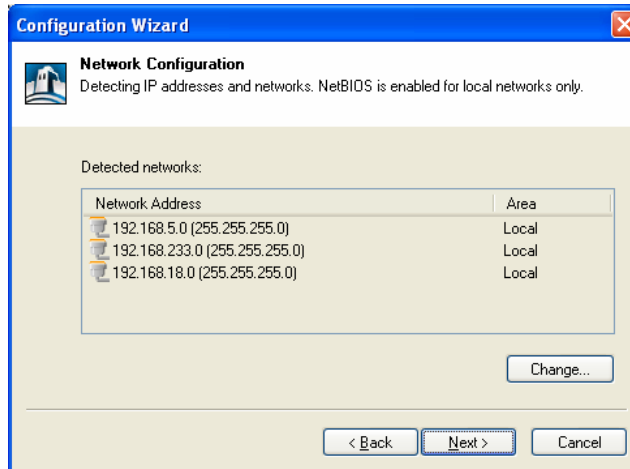
If you do not want to enable rules autcreation, select **Use predefined rules for detected applications** for the rule sets to be created according to our engineers' built-in presets in order to provide optimal system performance and application security.

After clicking **Next**, Outpost Firewall Pro automatically scans your system and adjusts all its settings without your supervision. It configures network settings, builds the Component Control database, and, in case you selected to use predefined rules, searches for known applications installed on your computer that might require Internet access and configures an appropriate the network access level for each of them.

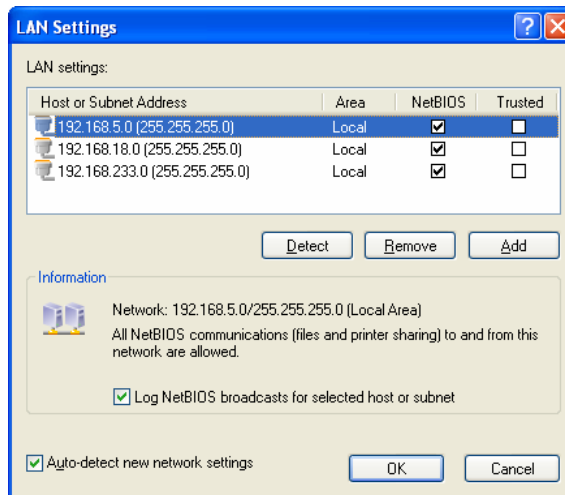
- **Custom Configuration.** If you select **Custom configuration**, the Configuration Wizard will guide you through the configuration process, allowing you to fine-tune the firewall for each of your specific needs, as well as select the specific configuration settings for each of the networks to which your system is connected and for each of your installed network-enabled applications. By modifying these configuration settings you can define the precise security levels that Outpost Firewall Pro provides. The wizard lets you produce a fully customized configuration, but it takes considerable time and assumes you have advanced knowledge of Windows and your system.

After clicking **Next**, the **Rules Autcreation** step (see above) is displayed allowing you to enable rules autcreation, so that rules for well-known applications and global rules are created automatically when each application first requires an action (for example, network access or process memory mdification). If you do not want to enable rules autcreation, select **Use predefined rules for detected applications** for the rule sets to be created according to our engineers' built-in presets to provide optimal system performance and application security.

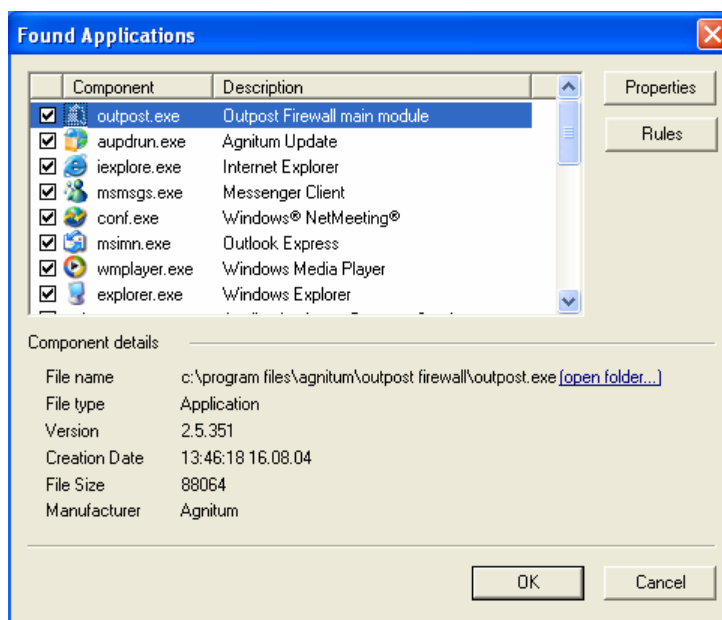
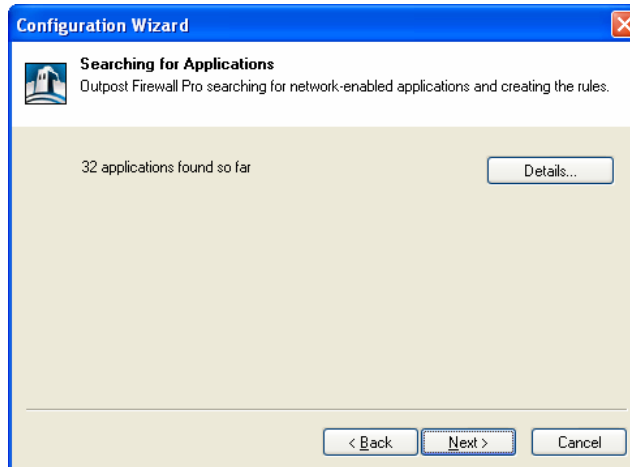
Click **Next** and Outpost Firewall Pro will automatically detect your network environment. On the **Network Configuration** step you will see a list of the networks to which your system is connected.



To view and edit the network settings, click the **Change** button. You can change these settings at any time when working with Outpost Firewall Pro. For details see the **5.5 System Level Filtering** chapter of Outpost Firewall Pro User Guide.



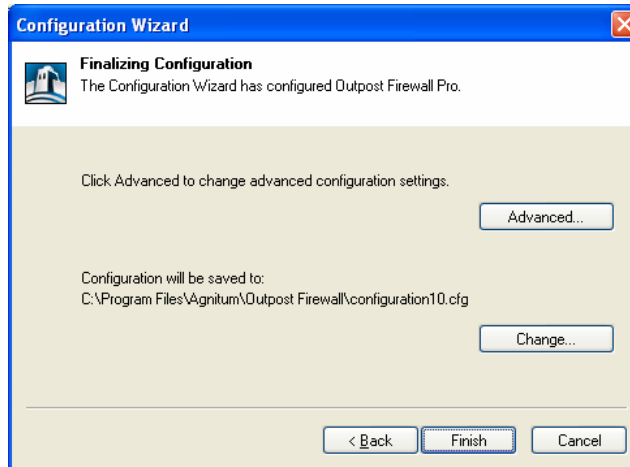
If you selected to use predefined rules, after clicking **Next**, Outpost Firewall Pro starts searching for the known applications installed on your computer, which might require Internet access, and configures a network access level for each of them. On the **Searching for Applications** step you can view a list of those applications and edit each suggested security rule using the **Details** button.



You can cancel rule configuration for a specific application by simply clearing the check box to the right of its name. Click **OK** to save and **Next** to proceed. You can change these settings at any time when working with Outpost Firewall Pro. See the **5.4 Creating Rules for Applications** chapter of Outpost Firewall User Guide for details.

After clicking **Next**, the Component Control database is collected and the wizard automatically proceeds to the last step.

On the final step you can configure other Outpost Firewall Pro settings, such as firewall policy, global rules, and others by clicking the **Advanced** button. The **Options** dialog then lets you alter any Outpost Firewall Pro settings. By default the created configuration is called **configurationN.cfg** (where N is an increasing index) and is saved in the Outpost Firewall Pro installation folder. If you prefer to save it to another location, click **Change** and specify its path.



Click **Finish** to apply the changes and save the configuration. You will be asked to reboot your system:



---

**IMPORTANT:** Do not launch **Outpost Firewall** manually using the **Start** button menu or Windows Explorer right after installing it. **You must reboot your computer** before **Outpost Firewall** can start to protect your system.

---

## 2 Uninstalling Outpost Firewall

To uninstall **Outpost Firewall**:

1. Right-click on **Outpost Firewall's** system tray icon and select **Exit**.
2. Click the Windows **Start** button and select **Control Panel > Add or Remove programs**.
3. Select **Agnitum Outpost Firewall** and click **Remove**.
4. Click **Yes** to confirm that you are going to uninstall the product and Windows Installer will perform all the necessary actions automatically whereupon you will be prompted to reboot the computer.

---

**Note:** To avoid software conflicts, **restart your system** after the uninstall process completes.

---

## 3 Keeping Your Protection Up-to-Date

With **Automatic Update**, you never have to be concerned about the latest Internet threats. **Outpost Firewall** provides you with a convenient way of keeping itself updated via the Internet. Each day, **Automatic Update** checks for newer components and plug-ins and if finds any, it retrieves them for you.

If, for some reason, you would like to check for newer components manually, you could run the update procedure by clicking on the **Update** button on **Outpost Firewall's** toolbar as shown here:



Alternatively, you could manually check for any updated components by performing the following steps:

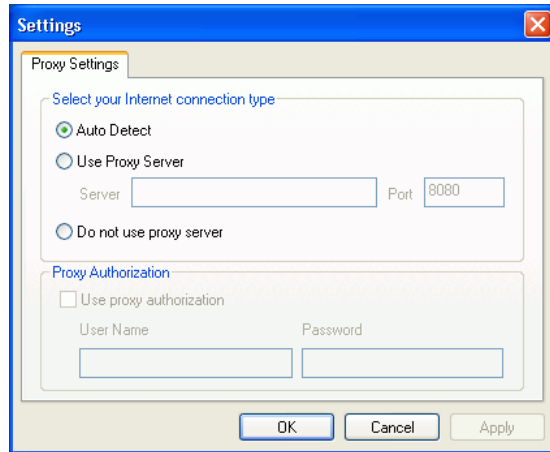
1. Click the **Start** button on Windows task bar.
2. Select **Programs**.
3. Then select **Outpost Firewall** from the **Agnitum** menu and click **Agnitum Update**.

Either of these two methods produces the following dialog:



The system will automatically find all the components to be updated.

Of course, components are updated only if updates are available for them. Clicking the **Settings** button displays the following dialog box:

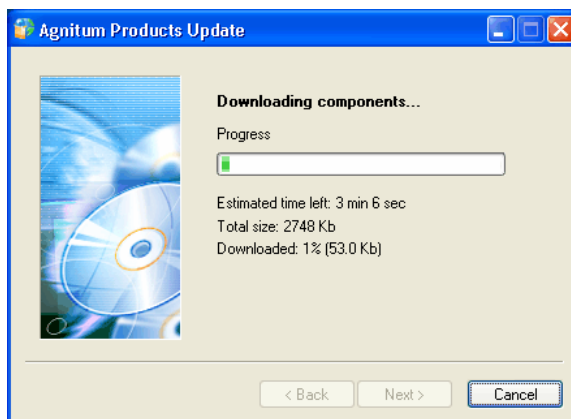


The options are:

- **Auto Detect** uses the proxy settings already specified in Microsoft Internet Explorer.
- **Use proxy server** lets you specify the parameters of the proxy server that is to be used by **Outpost Firewall's** Automatic Update. The **Server** and **Port** fields become visible when you select this option. Enter the name of your proxy server and its port number (port 8080 by default). If your proxy server requires authorization, select the appropriate check box and enter your username and password. If you are unsure what type of proxy you use or you do not know your username and password, please consult your system administrator.
- Select **Do not use proxy server** if your system is not connected to the Internet through a proxy server.

Click **OK** to save and **Next** to proceed.

Here is the next dialog showing the downloading progress:



When the download is complete, the last dialog is automatically displayed without you having to click the **Next** button:

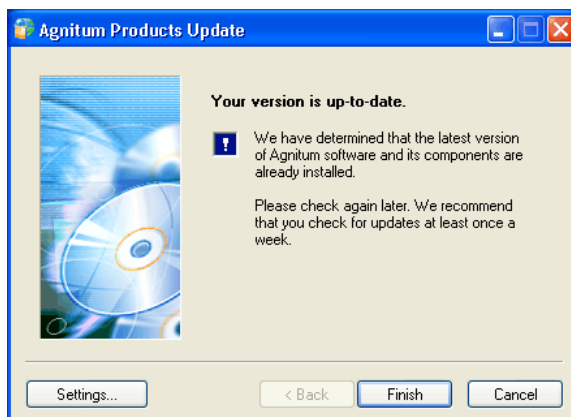


This dialog gives you the following choices:

- **Yes, I want to restart my computer now** to restart your computer immediately after you click **Finish**.
- **No, I will restart my computer later** gives you the opportunity of saving any incomplete work before restarting your computer. Be sure to restart your computer as soon as possible to take advantage of the increased protection afforded by the updated components you just downloaded.

**Note:** The Outpost updates take effect only after you reboot computer. If you simply restart Outpost, it still will use components of the older version. To see the list of component versions that Outpost uses, go to the **Help** menu and select **About > Modules**.

If there are no updates available, this dialog window is shown:



## 4 Log Database Maintenance

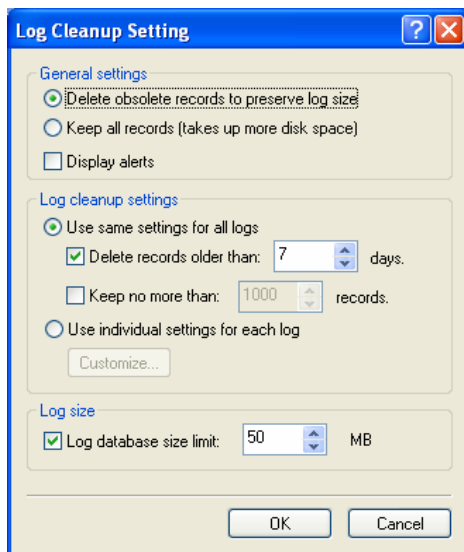
### 4.1 Database Cleanup

Outpost Firewall logs every activity it detects or performs, consequently the log database is continually growing. Eventually, the log database gets so large that it reduces logging performance as well as wastes disk space. In most cases, it is not necessary to log every Outpost event even if you intend to thoroughly analyze your network's activities.

Outpost Firewall features a **Log Cleaner** that maintains the log database at an optimum size.

The Log Cleaner automatically deletes obsolete, outdated events from the database to conserve disk space and maintain high logging performance.

To configure the Log Cleaner, open the **Outpost Log Viewer** and on the **File** menu click **Log cleanup settings**.



Select **Delete obsolete events to preserve the 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**.

**Log cleanup settings** allows you to set policies for the log cleanup. 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. You can either use the same settings for all logs or select to **Use individual settings for each log**.

**Log Cleaner** analyzes your settings to determine which will result in the smaller database size and then cleans the log to meet that setting's requirements.

For example, you specify to delete all records older than 5 days, keep 3000 records maximum and limit the log size to 7 megabytes. **Log Cleaner** checks the log and determines that keeping all records for the past 5 days results in a log size of 10 megabytes containing 4600 records for that period. Since the specified limit for the number of records (3000) is less than 4600, **Log Cleaner** computes the space required to keep 3000 records and evaluates it as 8 megabytes. Finally, **Log Cleaner** looks the evaluated size up against the specified database size limit (in this case, 7MB) and truncates the database to 7 megabytes containing only about 2600 records.

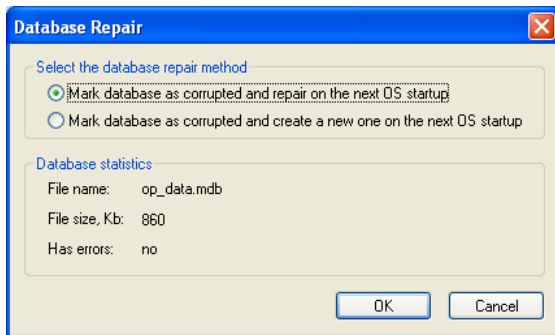
Select **Display alerts** to have the **Log Cleaner** display all notification messages during the cleanup process.

If you do not wish the **Log Cleaner** to delete any event records, select **Keep all records**. Note however that **Outpost Log Database** can grow significantly in size and it is not recommended that you disable the **Log Cleaner**.

**Tip.** To manually run the **Log Cleaner**, open the **Outpost Firewall** main window and press *F4*.

## 4.2 Repairing the Log Database

**Outpost Firewall's** log may become corrupted if your system crashes or shuts down unexpectedly. To restore the logging system, open the **Outpost Log Viewer** and select **Repair log database** on the **File** menu.



This dialog displays the current log database status: file name, size and whether or not the database has errors. If the database has no errors, but you experience logging problems it is recommended that you select **Mark database as corrupted and repair on the next OS startup** and click **OK** to have the logging system to attempt to repair the database after you restart Windows.

If this does not help, select **Mark database as corrupted and create a new one at the next OS startup** to have the logging system delete the current logging database and create a blank one after you restart Windows.

**Important:** In this case all the logging information will be lost.

## 5 Technical Support

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