

Maintenance
Guide

Outpost Security Suite 2007

Personal Security Software
from
Agnitum

Abstract

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

Table Of Contents

1	INSTALLING OUTPOST SECURITY SUITE	4
2	UNINSTALLING OUTPOST SECURITY SUITE.....	11
3	KEEPING YOUR PROTECTION UP-TO-DATE	12
4	LOG DATABASE MAINTENANCE.....	15
	4.1 DATABASE CLEANUP	15
	4.2 REPAIRING THE LOG DATABASE	16
5	TECHNICAL SUPPORT	17

1 Installing Outpost Security Suite

Outpost Security Suite's installation procedure is similar to that of most Windows programs.

Notes:

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

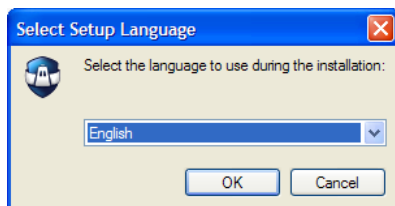
To start the installation program of the **Outpost Security Suite** system:

1. **Very Important!** Before installing **Outpost Security Suite**, uninstall any other security 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.

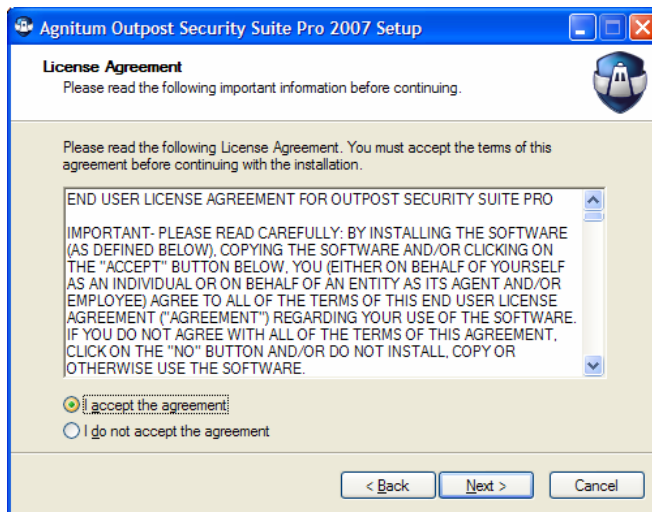


Choose the language for **Outpost Security Suite** interface and click **OK**. Setup will display the **Welcome** dialog that reminds you to close all running applications.

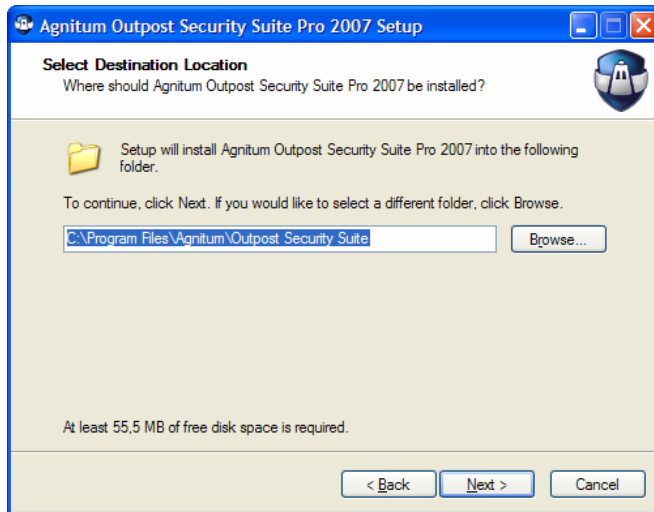


After clicking the **Next** button you will be asked to accept the License Agreement to use the **Outpost Security Suite**.

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:

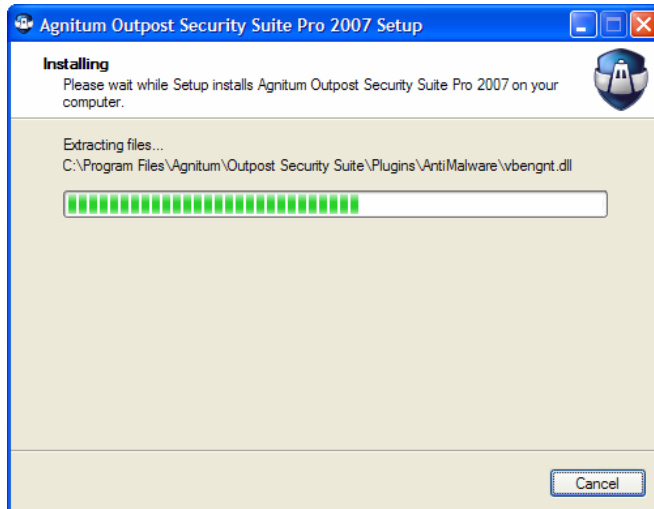


Click **Next** to proceed to the last step before actual installation:



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

The program displays the installation progress window:

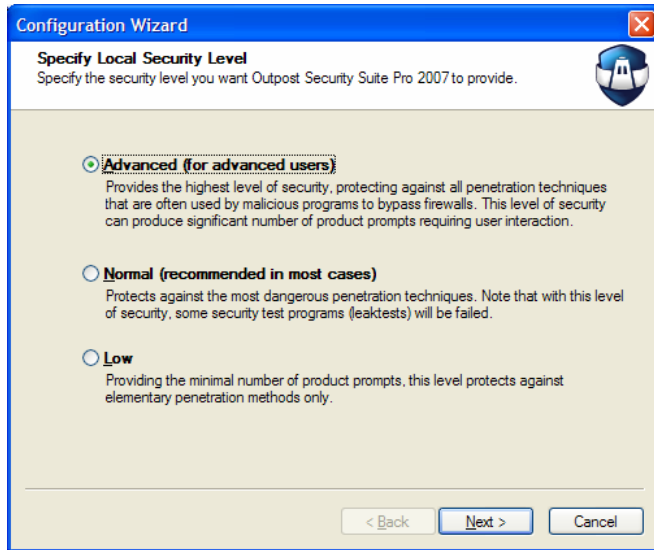


After the installation is finished, the **Configuration Wizard** will help you create a new configuration.

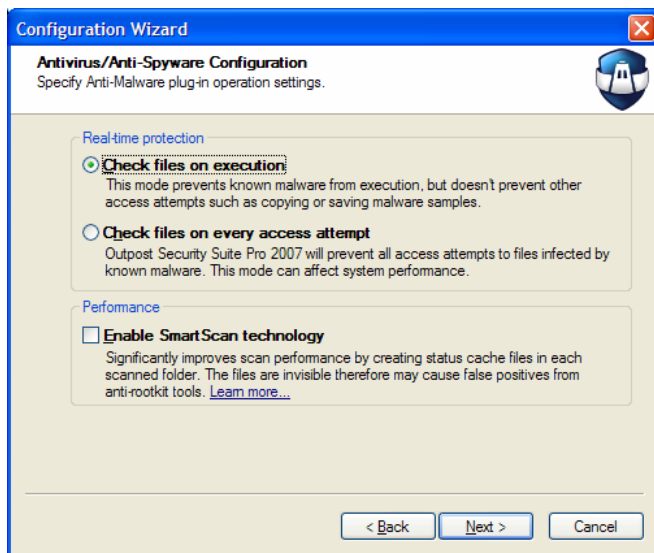
If you are installing over previous version, you can specify whether you want to preserve your configuration or create a new one from scratch.

If you select to create a new configuration, Configuration Wizard lets you select the local security level you'd prefer. The following levels are available (for details, see the userg guide):

- **Advanced**—provides the best protection against all penetration techniques that are often used by malicious software to bypass firewall software. Having selected this level, you will get a lot of product prompts that require your response; therefore it is recommended for advanced users.
- **Normal**—ensures protection against the more dangerous techniques only and is recommended for most cases. However, if Normal security level is selected, some of the more exotic security test programs (leaktests) will be failed.
- **Low**—provides protection against the easiest penetration techniques only; the number of product prompts is minimal.



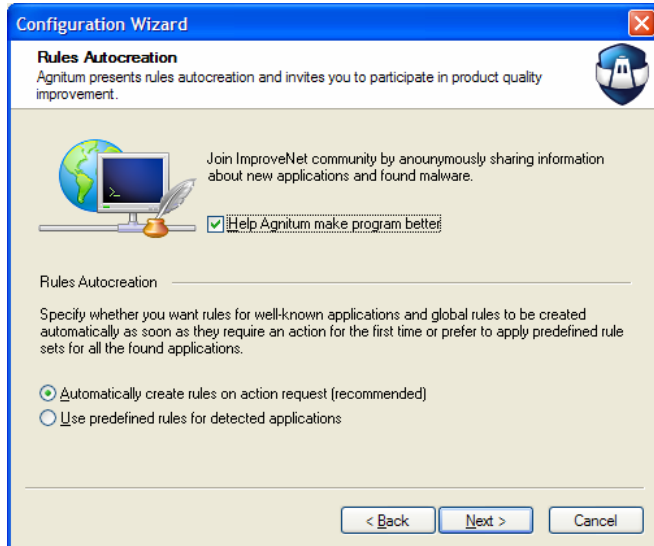
After you select the security level and click **Next**, the wizard allows you to specify Anti-Malware plug-in operation settings. Select **Check files on execution** if you want to prevent known malware from execution, but don't want to prevent other access attempts such as copying or saving malware samples. Or select **Check files on every access attempt** and Outpost Security Suite Pro will prevent all access attempts to files infected by known malware. Note, that the last mode can affect system performance.



You can also improve scan performance by setting Outpost Security Suite Pro to create status cache files in each scanned 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.

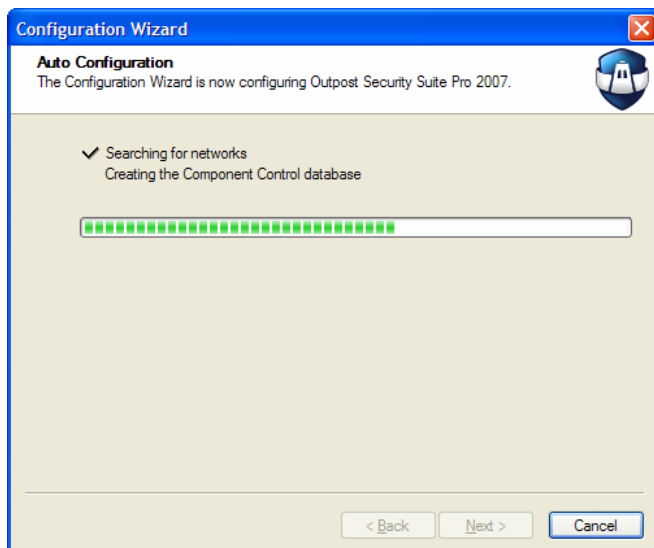
Click **Next** to proceed to the **Rules Autocreation** step, which allows you to enable rules autocreation, so that global rules and rules for well-known applications are created automatically when they first request an action (for example, network access or process

memory modification). If you do not want to enable rules autocreation, 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.

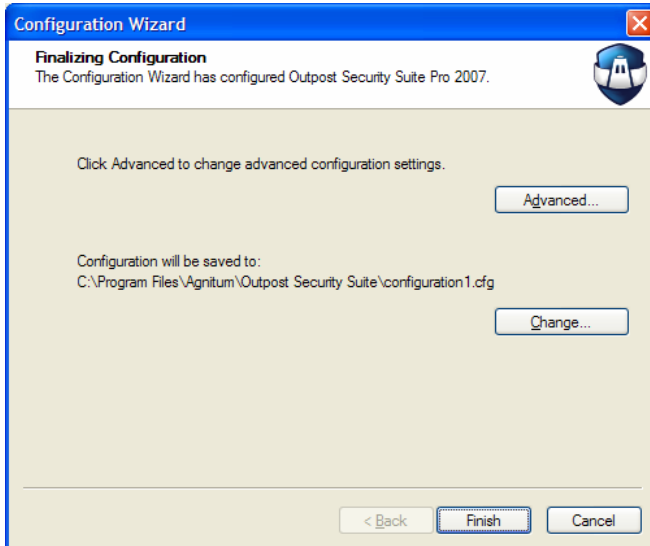


At this step, you can also join Agnitum ImproveNet program to improve quality, security and control features of products by selecting the **Help Agnitum make program better** check box.

After clicking **Next**, Outpost Security Suite 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.



Click **Next** to proceed to the last step where you can configure other settings, such as firewall policy, global rules, and others by clicking the **Advanced** button. The **Options** dialog then lets you alter any Outpost Security Suite Pro settings. By default the created configuration is called **configurationN.cfg** (where N is an increasing index) and is saved in the Outpost Security Suite 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 Security Suite** manually using the **Start** button menu or Windows Explorer right after installing it. **You must reboot your computer** before **Outpost Security Suite** can start to protect your system.

2 Uninstalling Outpost Security Suite

To uninstall **Outpost Security Suite**:

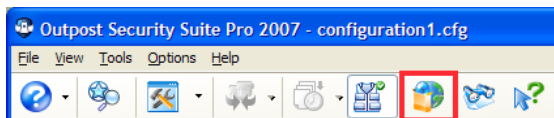
1. Right-click on **Outpost Security Suite**'s system tray icon and select **Exit**.
2. Click the Windows **Start** button and select **Control Panel > Add or Remove programs**.
3. Select **Agnitum Outpost Security Suite** and click **Remove**.
4. Click **Yes** to confirm that you are going to uninstall 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 Security Suite**vides 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 Security Suite's** toolbar as shown here:



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

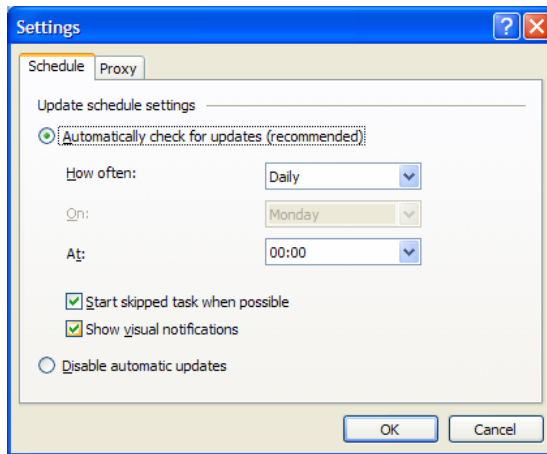
1. Click the **Start** button on Windows task bar.
2. Select **Programs**.
3. Then select **Outpost Security Suite** from the **Agnitum** menu and click **Agnitum Update**.

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:



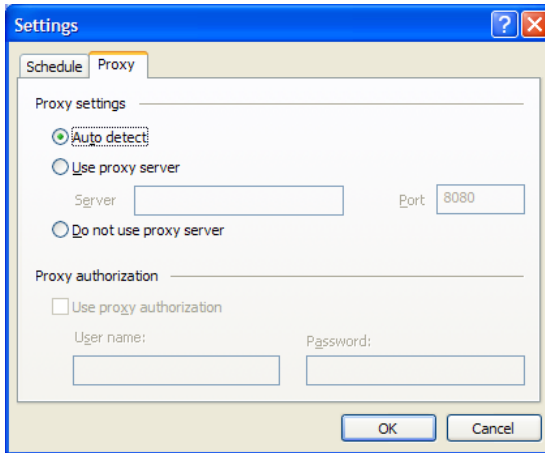
Automatic updates take place on a daily basis, however, you can choose time when your suite downloads updates on your own. To do this click the **Options** button on the toolbar and select **Update Settings**. On the **Schedule** tab you can enable automatic updates by selecting the **Automatically check for updates** or disable it by selecting **Disable automatic updates**.

When automatic updates option is on, you can choose how often the suite will download updates by selecting the frequency in the **How often** list. If you select weekly updates, you can also specify a day for updating and the exact time when the product will download updates; within daily updates you can specify the time of the day to download updates.

If for some reason your computer is switched off or does not have regular access to the Internet at the time specified for downloading updates, you can select the **Start skipped task when possible** check box, for the suite to start downloading updates as soon as your computer has Internet access.

Having selected the **Show visual notifications** check box, you will always know about the updating process.

If you connect to the Internet through a proxy server, you can set the connection settings on the **Proxy** tab. Auto detecting proxy server is a default option, but you can specify the server and port number explicitly. To do so, select **Use proxy server** under **Proxy settings** and type in the server name and port number in the text boxes provided.



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 connecting to the Internet your computer uses proxy server, but you want the updating process to be performed directly from the product developers' server, select **Do not use proxy server**.

If you do not use proxy server, you can select either **Do not use proxy server** or **Auto detect** option.

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

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**.

4 Log Database Maintenance

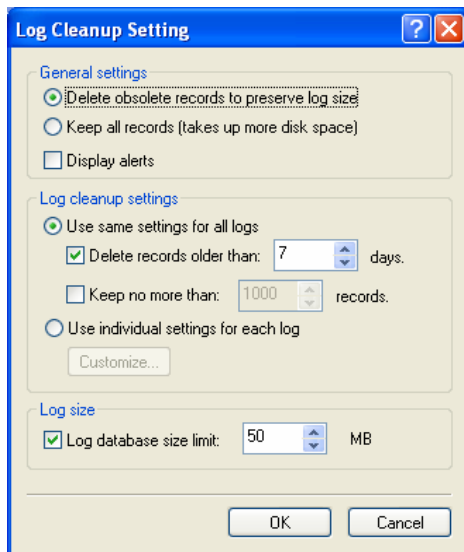
4.1 Database Cleanup

Outpost Security Suite 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 Security Suite 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.

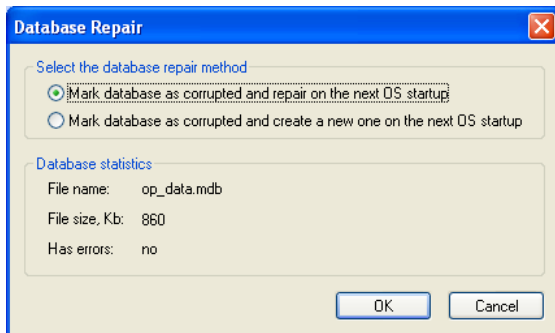
Select **Display alerts** to have the **Log Cleaner** display all notification messages during the cleanup process.

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 Security Suite** main window and press *F4*.

4.2 Repairing the Log Database

Outpost Security Suite'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 Security Suite, visit its support pages at <http://www.agnitum.com/support/> page for available support options including FAQs, Documentation, Forum, Tips-n-tricks and Troubleshooting.