Ad-Aware® 2007
User Manual

Table of Contents

Ad-Aware 2007 Overview

Using Ad-Aware 2007

Resources

What Is Ad-Aware 2007?

Ad-Aware 2007 is the latest version of Lavasoft's industry leading anti-spyware solutions. Ad-Aware 2007 allows you to combat the growing threats and latest advancements of malicious spyware and malware.

Ad-Aware 2007 protects you from spyware that secretly takes control of your computer, resulting in aggressive advertising pop-ups, sluggish computer activity and even identity theft through stolen private information. We give you the tools to detect hazardous content on your computer, clearly identify their threat level, and then give you the ability to remove unwanted content, so that your private information remains right where it should - under your control.

Lavasoft's advanced Code Sequence Identification (CSI) technology roots out deeply hidden malware and then searches for similar codes in order to identity emerging variants. Ad-Aware 2007 thoroughly scans your memory, registry, Hosts file, hard, removable and optical drives for known data-mining, aggressive advertising, parasites, scumware, keyloggers, trojans, dialers, malware, browser hijackers, and tracking components.

Ad-Aware 2007 Features

- Fully redesigned engine – provides optimal productivity with fast scans and top resource efficiency
- Advanced Code Sequence Identity technology – results in better detection of deeply imbedded and emerging malware
- Enhanced Detection Database – protects Ad-Aware 2007 users from more malware, with incremental and automatic updates resulting in fast download times
- New graphical user interface (GUI) - easy to navigate for beginners while maintaining advanced options for experienced users and businesses
- Multiple Browser Support – Internet Explorer, Firefox and Opera
- System Restore Point – provides a system restore point, particularly valuable for computer users who may have deleted a file in error during cleanup of their system

- Automatic scans and Web Updates – the all-new scheduler allows you to set a personalized schedule for automatic scans and Definitions File updates
- Ad-Watch TrackSweep – this new feature erases tracks left while surfing the Internet on Internet Explorer, Firefox and Opera, in one easy click of a button
- Hosts File Editor – allows users to add, delete or make changes to the Hosts File to create Web navigational shortcuts and block specific sites

Ad-Aware 2007 System Requirements

Processor: P600

RAM: Operating system + minimum 50 MB (100 MB recommended)

Hard Disk: 50 MB free space recommended

Operating Systems:

Windows 2000 (Pro and Server)
Windows Server 2003
Windows XP (Home, Pro, Editions)
Windows Vista (32 bit)

Web Browser: Internet Explorer (version 5.5 or higher), Firefox (version 1.5 or higher), or Opera (version 9 or higher)

Install Ad-Aware 2007

For specific questions related to your download or purchase of Ad-Aware 2007, please log in to the Support Center at www.lavasoft.com.

If you are installing Ad-Aware 2007 on Windows 2000 or XP operating systems, please make sure you have administrative rights. Ad-Aware 2007 is a service and as such has escalated rights. You must have administrative rights in order to install Ad-Aware 2007. If you are unsure if you have the necessary permission, please contact your system administrator or refer to your computer's user guide before installing.

Start Installation

If you are installing Ad-Aware 2007 from a CD, insert the CD into the CD-ROM drive. If you downloaded your copy of Ad-Aware 2007, locate and double-click on the downloaded file to start the installation.

Uninstall Previous Versions of Ad-Aware

Ad-Aware 2007 will not function correctly if old versions are not removed prior to installing a new version or an upgrade. When you proceed with the installation of Ad-Aware 2007, all prior Ad-Aware versions will automatically uninstall.

Welcome Screen

Please read the License Agreement before you proceed. When you have completed reviewing the agreement and if you agree to the terms, select the button next to "I accept the license agreement" and press "Next" to continue with the installation of the software.

Destination Location

Click "Next" to accept the default location or use "Browse" to specify where you want Ad-Aware 2007 installed.

Start Installation

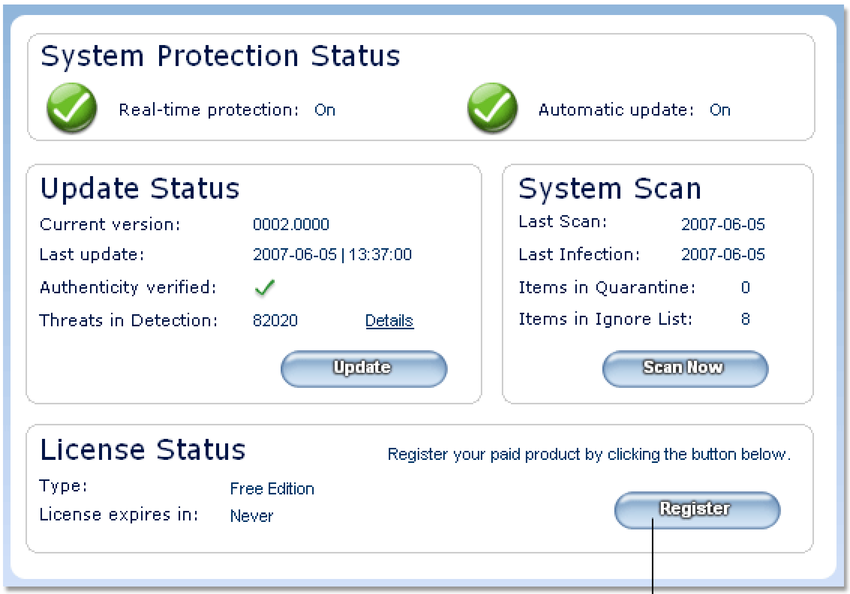
Click "Next" to begin installing Ad-Aware 2007 onto your computer. After the files finish copying, you will receive a confirmation message that the installation was successful.

Installation Successful

Click "Finish" to complete the installation process.

Registering Your Product

If you have bought Ad-Aware 2007 Plus or Pro you will need to register your product in order to use its extended functionality.The registration is accessed from the main status screen:



System Protection Status

Real-time protection: On

Automatic update: On

Update Status

Current version: 0002.0000

Last update: 2007-06-05 | 13:37:00

Authenticity verified: ✓

Threats in Detection: 82020

System Scan

Last Scan: 2007-06-05

Last Infection: 2007-06-05

Items in Quarantine: 0

Items in Ignore List: 8

License Status

Register your paid product by clicking the button below.

Type: Free Edition

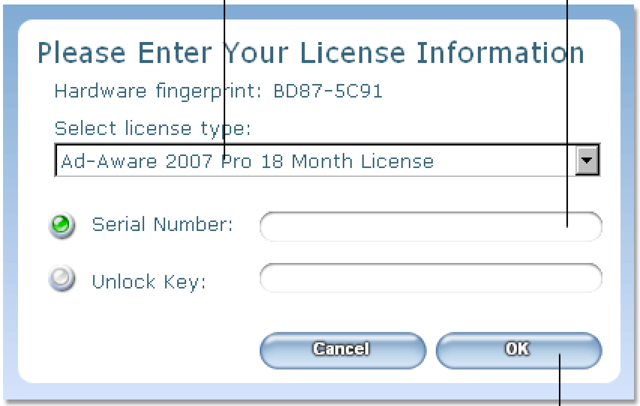
License expires in: Never

Click the Register button to open the registration window.

In the License Information Window

Choose the license version you have purchased from the drop-down menu.

Enter the serial number for your product in the Serial Number box.



Please Enter Your License Information

Hardware fingerprint: BD87-5C91

Select license type:

Ad-Aware 2007 Pro 18 Month License

● Serial Number:

○ Unlock Key:

Press OK and Ad-Aware 2007 will connect to the Internet to verify your registration. When the verification process is complete the window will close.

The Interface of Ad-Aware 2007

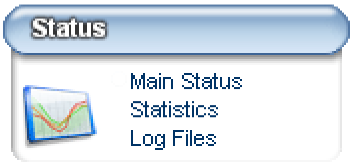
Quick Launch Menu

Opens copyright and contributor information about Ad-Aware 2007.

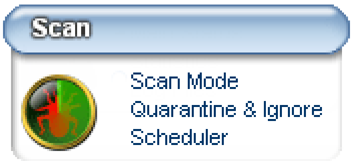
Opens the Ad-Aware 2007 Product Manual.

Main Menu

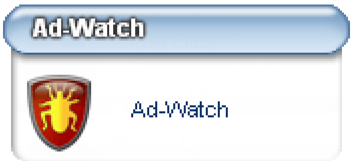
Click the main menu buttons on the interface to open the drop-down menu in each section.



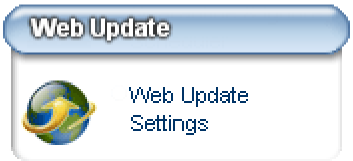
View the status of the components that make up Ad-Aware 2007, statistics from your scans, and log files from your scans.



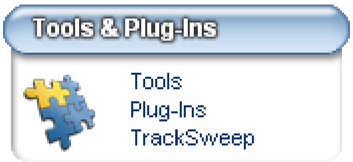
Perform spyware scans, manage your Quarantine and Ignore lists, and use the Scheduler Plus Pro to set up automatic scans and Web Updates.



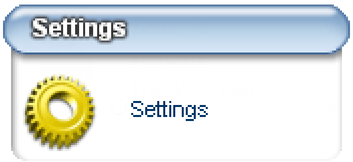
Launch the Ad-Watch real-time monitor. Plus Pro



Use Web Update to keep Ad-Aware 2007's threat database up-to-date with the latest Definitions File, and to receive software updates.



Choose additional privacy and protection options like the stand alone tools Process Watch Pro and Hosts File Editor Plus Pro , Ad-Aware 2007 plug-ins, and the convenient TrackSweep feature.



Change the Ad-Aware 2007 settings to fit your individual needs.

First Step Settings

Before you scan your computer with Ad-Aware 2007 for the first time, use Web Update to make sure that you are using the latest Definitions File and software version updates.

To stay protected from the latest threats, it is important that you regularly update Ad-Aware 2007's threat database, the Detection Database, with the latest Definitions File update. Regular scans are highly recommended.

The Scheduler feature allows you to manage Ad-Aware 2007 by setting up automatic scans and Web Updates to take place on scheduled dates and at specific times.

We also recommend having Ad-Aware 2007 set to automatically quarantine files prior to removal. You can set up Ad-Aware 2007 to automatically perform Web Updates, scan, remove infections, and quarantine detected objects. In order to make these adjustments, follow the instructions below.

Automatic Web Update

Use the Scheduler to schedule automatic Web Updates to occur at set times. To open the Scheduler, click the "Scan" menu button and then click "Scheduler" in the drop-down menu. Click "Add," select "Web Update" from the list of tasks, and then specify the frequency, date and time for the Web Update to occur. (More information is available in the "Using Ad-Aware 2007" chapter, under "Scheduler".)

You can also adjust Ad-Aware 2007 settings to automatically update the Detection Database prior to scanning your computer. Click the "Settings" button to open the Ad-Aware 2007 settings menu. Select the "Auto Scans" tab. Under "System," check the box next to "Update Definitions File before scanning." If an updated file is available, it will automatically be downloaded to your computer before scanning. Click "Save" to save your changes.

Automatic Scans

Use the Scheduler to schedule automatic scans to occur at set times. To open the Scheduler, click the "Scan" menu button and then click "Scheduler" in the drop-down menu. Click "Add," select "Smart Scan" or "Full Scan" from the list of tasks, and then specify the frequency, date and time for the scan to occur. (More information is available under the "Using Ad-Aware 2007" chapter, under "Scheduler".)

You can also adjust the Ad-Aware 2007 settings to automatically scan your computer when Ad-Aware 2007 is launched. Select the "Auto Scans" tab. Under "Start-Up Scan," select a scan mode. Click "Save" to save your changes.

Automatic Cleaning

You can change the Ad-Aware 2007 settings so that threats detected on your system after a scan with a certain TAI (Threat Analysis Index) level are automatically removed from your system. Select the "Auto Scans" tab. Under "System," select a setting in the "Automatically remove infection with TAI higher than 'X'." Click "Save" to save your changes.

Automatic Quarantine

You can change the Ad-Aware 2007 settings so that detected threats are automatically quarantined prior to being removed from your system. Select the "Auto Scans" tab. Under "Safety," check the box next to "Quarantine objects prior to removal." Click "Save" to save your changes.

Status

Click the "Status" menu button to open the drop-down Status menu. Click "Main Status" in the drop-down menu to see the Ad-Aware 2007 Main Status screen, Statistics, and Log Files.

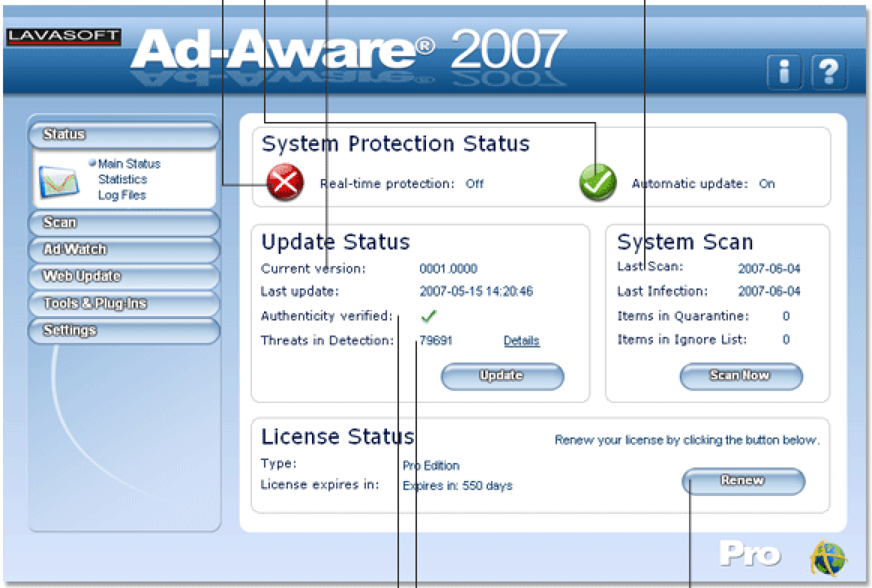
Main Status Screen

Shows if you have set up automatic Web Updates with the Scheduler.

Shows if the Ad-Watch real-time monitor is activated.

Shows the version of the Definitions File that you are using.

Shows information about previous scans with Ad-Aware 2007. Click "Scan Now" to navigate to the "Scan Mode" screen to begin a scan.



System Protection Status

Real-time protection: Off

Automatic update: On

Update Status

Current version: 0001.0000

Last update: 2007-05-15 14:20:46

Authenticity verified: ✓

Threats in Detection: 79691

System Scan

Last Scan: 2007-06-04

Last Infection: 2007-06-04

Items in Quarantine: 0

Items in Ignore List: 0

License Status

Renew your license by clicking the button below.

Type: Pro Edition

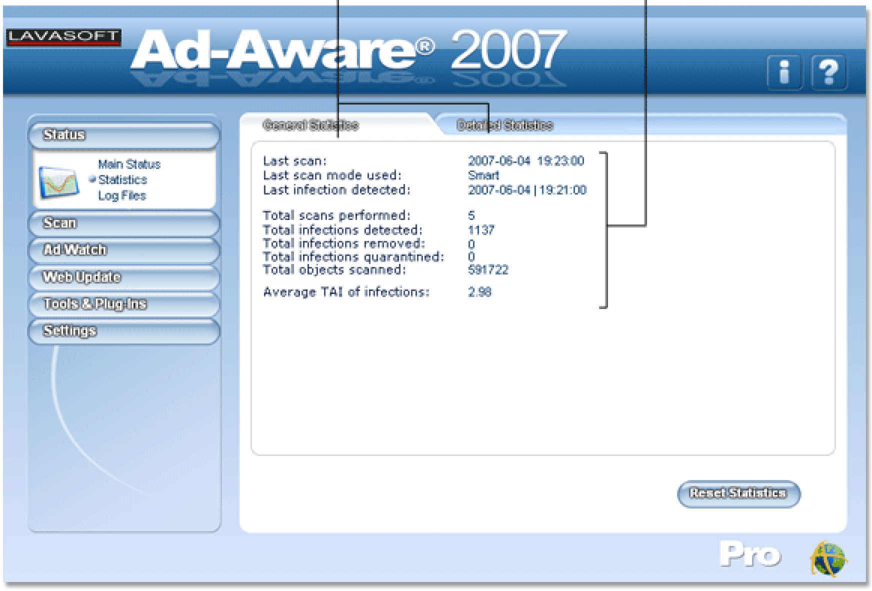
License expires in: Expires in: 550 days

SSL updates mean that you are assured an authentic file. If your screen shows a red "X" instead of a green checkmark, or if you receive a warning that the Definitions File is corrupt, the file could not be loaded; make sure to run a Web Update to download the latest Definitions File.

Shows the number of threats currently in Lavasoft's Detection Database. Click "Details" to see the number of families, fingerprints and registry entries that make up the Detection Database.

Shows your current license information. Click "Renew" to purchase a new license for Ad-Aware 2007 from Lavasoft's website.

General Statistics



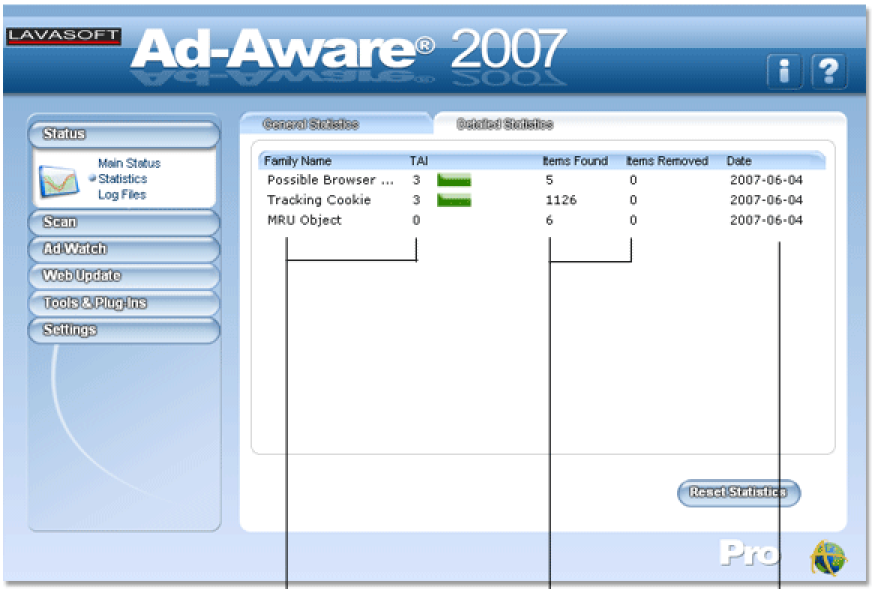
Last scan:	2007-06-04 19:23:00
Last scan mode used:	Smart
Last infection detected:	2007-06-04 | 19:21:00
Total scans performed:	5
Total infections detected:	1137
Total infections removed:	0
Total infections quarantined:	0
Total objects scanned:	591722
Average TAI of infections:	2.98

Statistics from your past scans are filed here. Use the tabs to view General and Detailed Statistics.

Shows total numbers since you installed Ad-Aware 2007 or since you last reset the statistics.

Detailed Statistics

Shows in-depth statistics about the objects detected in past scans.



Family Name	TAI		Items Found	Items Removed	Date
Possible Browser ...	3	🟩	5	0	2007-06-04
Tracking Cookie	3	🟩	1126	0	2007-06-04
MRU Object	0		6	0	2007-06-04

Shows the type of objects detected in past scans and their TAI - Threat Analysis Index

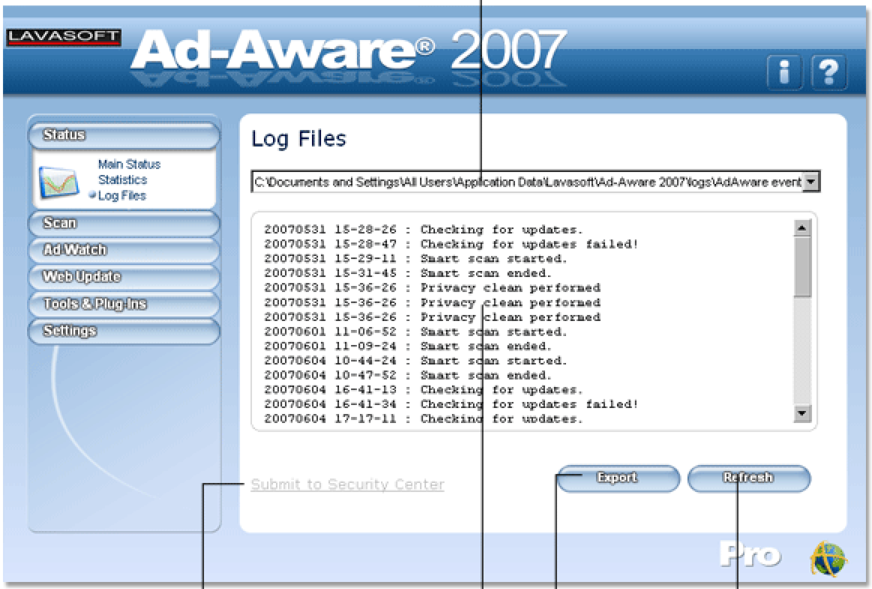
Shows the total number of objects in that category that were found and the total number you chose to have Ad-Aware 2007 remove.

Shows the date you performed your last scan.

Log Files

Records of the action that occurred when you performed a scan. Under "Settings" you can adjust the amount of log files to create, type of information to include, and where to save the files.

Use the drop-down menu to select a log file.



C:\Documents and Settings\All Users\Application Data\Lavasoft\Ad-Aware 2007\logs\AdAware event

```
20070531 15-28-26 : Checking for updates.
20070531 15-28-47 : Checking for updates failed!
20070531 15-29-11 : Smart scan started.
20070531 15-31-45 : Smart scan ended.
20070531 15-36-26 : Privacy clean performed
20070531 15-36-26 : Privacy clean performed
20070531 15-36-26 : Privacy clean performed
20070601 11-06-52 : Smart scan started.
20070601 11-09-24 : Smart scan ended.
20070604 10-44-24 : Smart scan started.
20070604 10-47-52 : Smart scan ended.
20070604 16-41-13 : Checking for updates.
20070604 16-41-34 : Checking for updates failed!
20070604 17-17-11 : Checking for updates.
```

Click to send your log file to Lavasoft's Security Center.

Contains information about your scan like the settings used, objects detected, and the processes that were running on your computer during the scan.

Click to save the log file to a specific location.

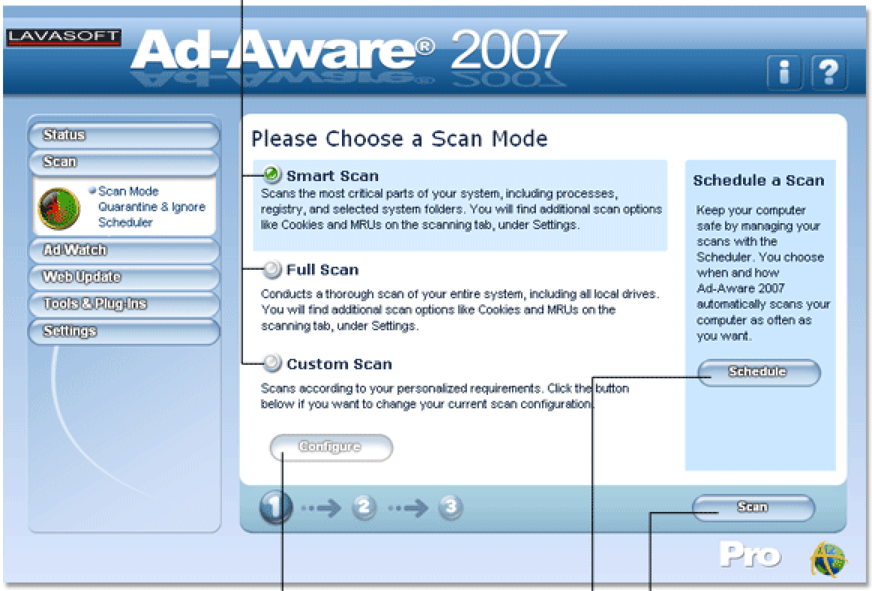
Click to update the content of the selected file.

Scan

Click the "Scan" menu button to open the "Scan Mode" screen, where you can choose the type of scan you would like to perform- a Smart Scan, Full Scan, or Custom Scan. Before you scan your computer, you should always be sure to have the most recent Definitions File by performing a Web Update. See more information about each scan mode below.

Choose A Scan Mode

Click to select a scan mode.



Please Choose a Scan Mode

Smart Scan
Scans the most critical parts of your system, including processes, registry, and selected system folders. You will find additional scan options like Cookies and MRUs on the scanning tab, under Settings.

Full Scan
Conducts a thorough scan of your entire system, including all local drives. You will find additional scan options like Cookies and MRUs on the scanning tab, under Settings.

Custom Scan
Scans according to your personalized requirements. Click the button below if you want to change your current scan configuration.

Schedule a Scan
Keep your computer safe by managing your scans with the Scheduler. You choose when and how Ad-Aware 2007 automatically scans your computer as often as you want.

Select Custom Scan and click to choose specific sections and directories that you want Ad-Aware 2007 to scan.

Click to open the "Schedule Task" window to set up a scheduled scan.

After choosing a scan mode, click to have Ad-Aware 2007 begin to scan your system.

Smart Scan

The Smart Scan is a fast system check that scans only the most critical sections of your system. The Smart Scan will scan your memory, registry, cookies, favorites, and Hosts file. The directories scanned are Windows, Temp and Program Files. The Smart Scan does not scan archived content.

This scan mode should only be used for daily system maintenance; use this scan if you are sure that your system is clean and you have performed a Full Scan or an in-depth Custom Scan on your main hard drive at least once during the past month. If this is your first scan, you suspect that your system has become infected with suspicious content, or you have used another anti-spyware product prior to installing and using Ad-Aware 2007, we recommend performing a Full Scan.

Full Scan

The Full Scan is an in-depth scan mode that thoroughly scans your entire system including all local drives. We recommend using the Full Scan when you use Ad-Aware 2007 for the first time, and at regular intervals to ensure that your system is clean.

The Full Scan takes longer to scan your system than the Smart Scan, but is more likely to find infections that have been installed on drives other than your main hard disk or in your archives. In addition to the areas scanned during a Smart System Scan, all fixed drives and archive files are also scanned.

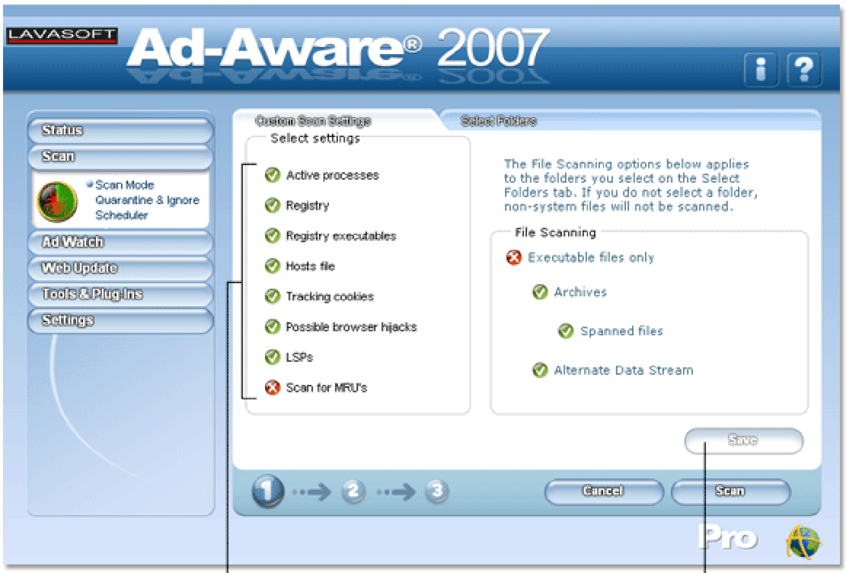
Custom Scan Plus Pro

The Custom Scan scans your system using your pre-configured settings. You can customize Ad-Aware 2007 to scan specific sections or directories.

Custom Scan Settings - Sections

Custom Scan Settings

After clicking "Configure," choose from the following customized scan settings. See a description of each section you can choose to scan below.



Select settings

✓ Active processes
✓ Registry
✓ Registry executables
✓ Hosts file
✓ Tracking cookies
✓ Possible browser hijacks
✓ LSPs
☒ Scan for MRU's

The File Scanning options below applies to the folders you select on the Select Folders tab. If you do not select a folder, non-system files will not be scanned.

File Scanning

☒ Executable files only
✓ Archives
✓ Spanned files
✓ Alternate Data Stream

Check the boxes to choose sections to scan during custom scans.

Click to save your settings to use when you perform customized scans.

Sections to Scan

Active processes	Scans all active processes currently running on your system.
Registry	Scans known spyware areas of the registry for the current user.
Registry executables	Scans within the registry for malicious executables.
Hosts file	Scans your Hosts file. Edits to the Hosts file may occur due to home page hijackers. If you use a Hosts file editor to block content, this option can cause some entries to be detected and presented for removal. To avoid any unwanted changes to your Hosts file, please review the content at the end of a scan and select the entries that you want to ignore in subsequent scans.
Tracking cookies	Scans for tracking cookies in Internet Explorer, Mozilla Firefox, and Opera.
Possible browser hijacks	Scans browser settings (like start page and search page), favorites, and desktop for malicious URLs.
LSPs	Detects and unloads malicious LSP (Layered Service Providers). LSP are used by malicious software to detect network activity. The LSPs must be loaded for Ad-Aware to detect them.
Scan for MRUs	Scans lists of Most Recently Used objects.

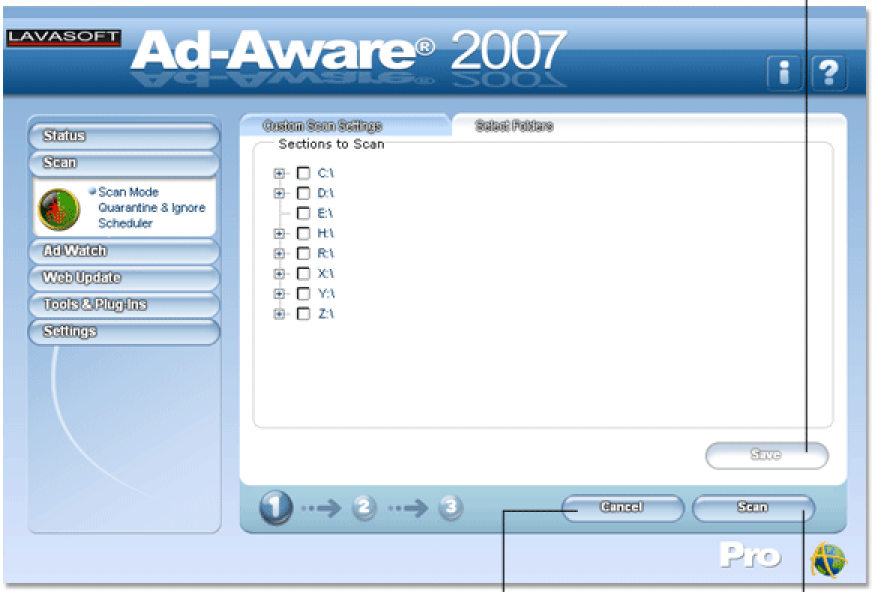
File Scanning

Executable files only	Scans only for executable files. This option should be used by advanced users because this will eliminate detection of related content that could cause the removed executables to be reinstalled at a later time.
Archives	Scans within archives such as .zip, .cab, etc.
Spanned files	Scans CAB files which are spanned. Spanned CABs occur where several CAB files make up a single CAB archive.
Alternate Data Stream (ADS)	Scans files and simultaneously investigates ADS streams for malicious objects.

Custom Scan Settings - Files & Folders

Select Folders

Click the "Select Folders" tab to select folders and directories you want to scan.



Select the directories you want to scan and click here to save your settings.

Click to go back to the "Choose a Scan" screen

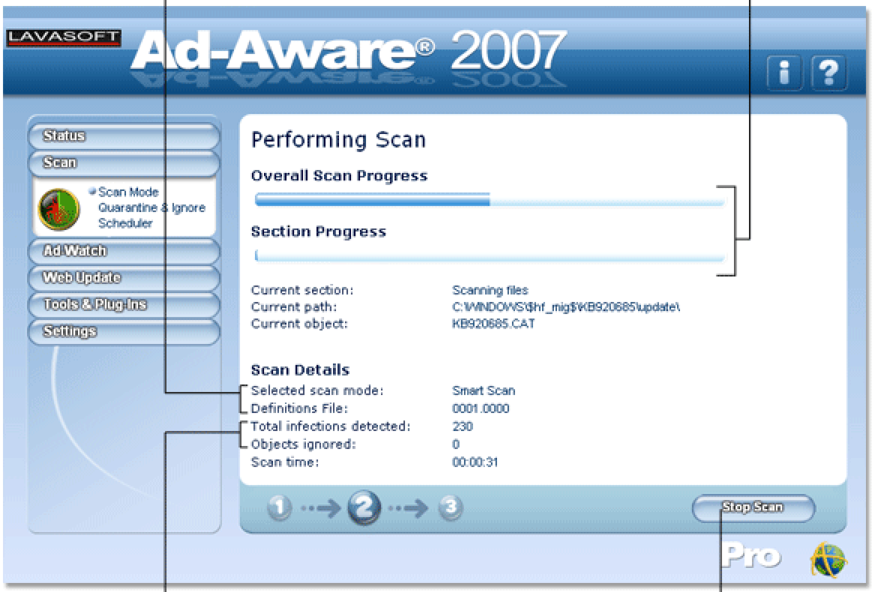
After you have selected the areas you want to scan, click to start your custom scan.

Performing Scan

After you select a scan mode and click "Scan", Ad-Aware 2007 will begin to scan your system, and the "Performing Scan" screen will appear.

Shows the type of scan you chose to perform and the Defintions File you are using.

Actively shows the scan's progress.



Performing Scan

Overall Scan Progress

Section Progress

```
Current section:            Scanning files
Current path:               C:\WINDOWS\$hf_mig$\KB920685\update\
Current object:             KB920685.CAT
```

Scan Details

```
Selected scan mode:         Smart Scan
Definitions File:           0001.0000
Total infections detected:  230
Objects ignored:            0
Scan time:                  00:00:31
```

Actively shows infections as they are detected and objects that have been ignored.

Click to stop the scan. You will see the results from the sections that were scanned.

Note! Virus Warnings

While performing a scan with Ad-Aware 2007, a background anti-virus monitor (from another provider) may issue an alert, stating that a virus has been found in the temporary directory (%temp%) for the current user. This does not necessarily mean your computer has been infected with an active virus.

Most anti-virus resident scanners will not scan compressed files and only monitor your memory for signs of an active viral process. During a scan, Ad-Aware 2007 will temporarily decompress files to scan their contents without activating the content, but in doing so, the file is noticed by the anti-virus' resident scanner. Also, some anti-virus applications include an option to quarantine infected files, and when Ad-Aware 2007 decompresses these quarantined files, the anti-virus background scanner detects the virus moving outside the quarantine area.

To avoid this, you can either remove the quarantined files through your anti-virus application, or have Ad-Aware 2007 ignore the anti-virus program's quarantine folders/files during a scan.

Scan Results

After the scan is complete, you will be presented with a detailed listing of the items that were detected in the "Scan Results" screen. Please review each detected item in the results screen before removing it. We do not suggest or recommend that everything detected by Ad-Aware 2007 should be removed. You have the final say in what to delete from your system.

Ad-Aware 2007 is designed to report possible suspicious content on your system, give you a straightforward method to understand the content detected, and then provide a simple way to remove threats.

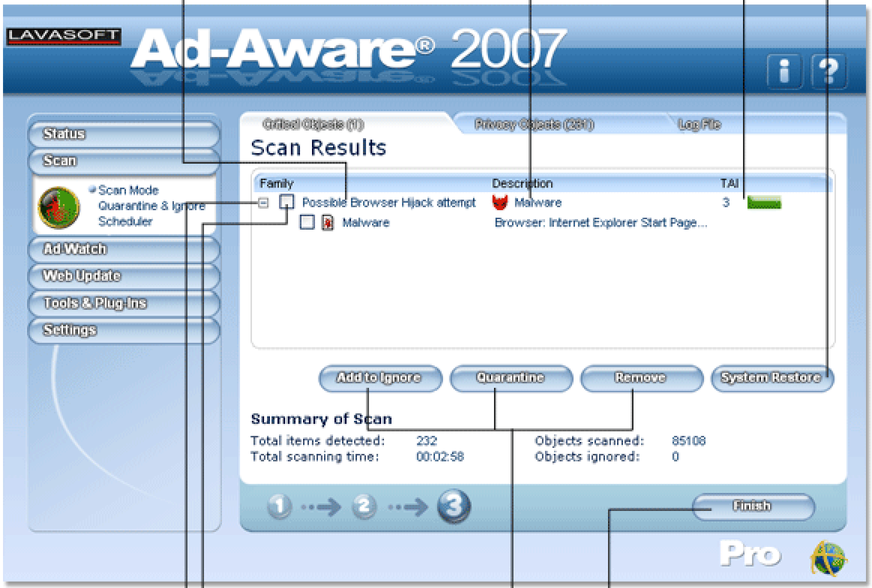
In the Scan Results screen, detected objects are separated into critical objects and privacy objects. The total number of critical objects and privacy objects detected during the scan are listed at the top of each tab.

Shows the family name of the objects.

Shows the category that Lavasoft has classified that threat to be in. Hold the mouse over an object to see a description of it.

Click to set a Windows system restore point

Shows the threat's TAI (Threat Analysis Index) level.



Scan Results

Family	Description	TAI
⊟ □ Possible Browser Hijack attempt	Malware	3
□ Malware	Browser: Internet Explorer Start Page...	

Summary of Scan

Total items detected:	232	Objects scanned:	85108
Total scanning time:	00:02:58	Objects ignored:	0

Click to expand the list to see all detected objects in this family.

Click to select all objects detected in this family.

For each detected critical object, you can choose to add it to the Ignore List, Quarantine it, or remove it from your system by checking the box beside the object(s) and then clicking one of these buttons.

After you have reviewed and handled all detected infections (objects can only be added to the Ignore List and Quarantine from this screen), click to exit this screen and view your "Scan Summary."

Critical Objects

Critical objects are detected objects that may pose a threat and should be considered for removal.

In order to give you information about each critical object detected, items are grouped under their family name, and are listed with their category, assigned Threat Analysis Index (TAI) level, and file path.

The Threat Analysis Index (TAI) associated with each detected object enables you to easily understand what constitutes an annoying threat and what should be recognized as a high risk to your privacy and security. The TA point system is based on a 10-point scale, with 1 representing the lowest threat and 10 representing the highest.

More information is available in the Resources chapter on the Threat Analysis Index, or in the Lavasoft Security Center. (The Threat Analysis Index was previously known as the Threat Assessment Chart).

For each detected critical object, you can choose to:

Add to Ignore: Add the object to the Ignore List; keep the item on your system and make sure it is not detected in future scans.

Quarantine: Add the object to the Quarantine; isolate and back-up the object in quarantine, where it does not pose a threat to your system.

Remove: Delete the object from your system.

You can either select each object individually by checking the box beside it, or use the selection options in the context menu.

Before deleting critical objects, you have the option to create a system restore point. A system restore point allows you to restore your computer to a previous working state, in the event of a problem. System restore creates backups, or restore points, of vital system configurations and files. You may choose to create a system restore point prior to deleting objects that you are unsure of removing, or after handling items detected by a scan, when you know that your system is clean.

Critical Objects Context Menu

Right-click within the "Critical Objects" section of the "Scan Results" screen to open the context menu where you can choose from the following operations:

- Select All Objects: Select all of the detected critical objects.
- Unselect All Objects: Unselect all of the detected critical objects.
- Add Selected to Ignore List: Add all of the selected critical objects to the Ignore List.
- Quarantine Selected: Add all of the selected critical objects to the Quarantine

Privacy Objects

Privacy objects consist of tracking cookies and MRU (Most Recently Used) lists. These objects are not considered to be a critical threat to your security, but they may be removed if you desire.

For each detected privacy object, you can choose to:

Add to Ignore: Add the object to the Ignore List; keep the item on your system and make sure it is not detected in future scans.

Remove: Delete the object from your system.

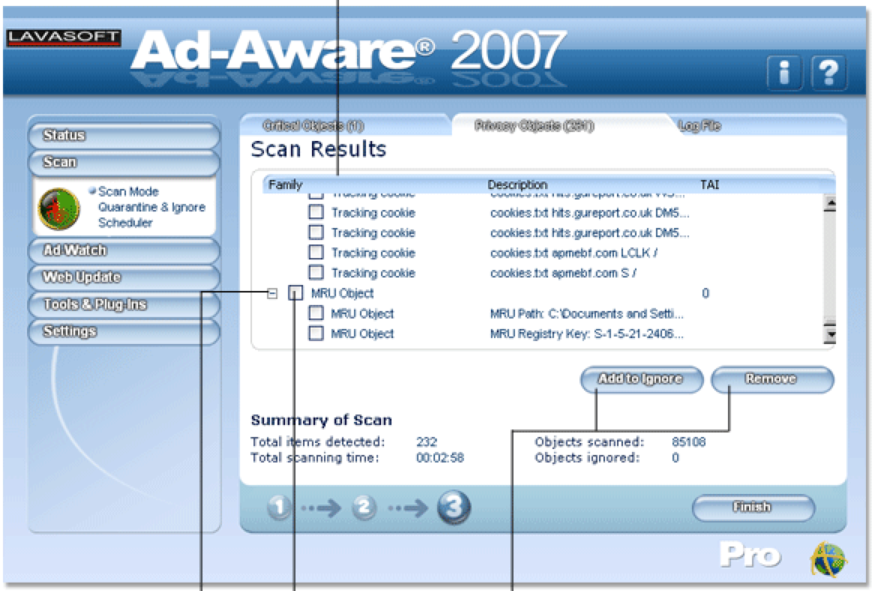
You can either select each object individually by checking the box beside it, or use the selection options in the context menu.

Privacy Objects Context Menu

Right-click within the "Privacy Objects" section of the "Scan Results" screen to open the context menu where you can choose from the following operations:

- Select All Objects: Select all of the detected privacy objects.
- Unselect All Objects: Unselect all of the detected privacy objects.

Shows the category that Lavasoft has classified that threat to be in. Double-click on the category to see a description of it.



Scan Results

Family	Description	TAI
□ Tracking cookie	cookies.txt hits.gureport.co.uk DM5...	
□ Tracking cookie	cookies.txt hits.gureport.co.uk DM5...	
□ Tracking cookie	cookies.txt apmebf.com LCLK /	
□ Tracking cookie	cookies.txt apmebf.com S /	
⊟ □ MRU Object		0
□ MRU Object	MRU Path: C:\Documents and Setti...	
□ MRU Object	MRU Registry Key: S-1-5-21-2406...	

Summary of Scan

Total items detected: 232
Total scanning time: 00:02:58
Objects scanned: 85108
Objects ignored: 0

Click to expand the list to see all detected objects in this category.

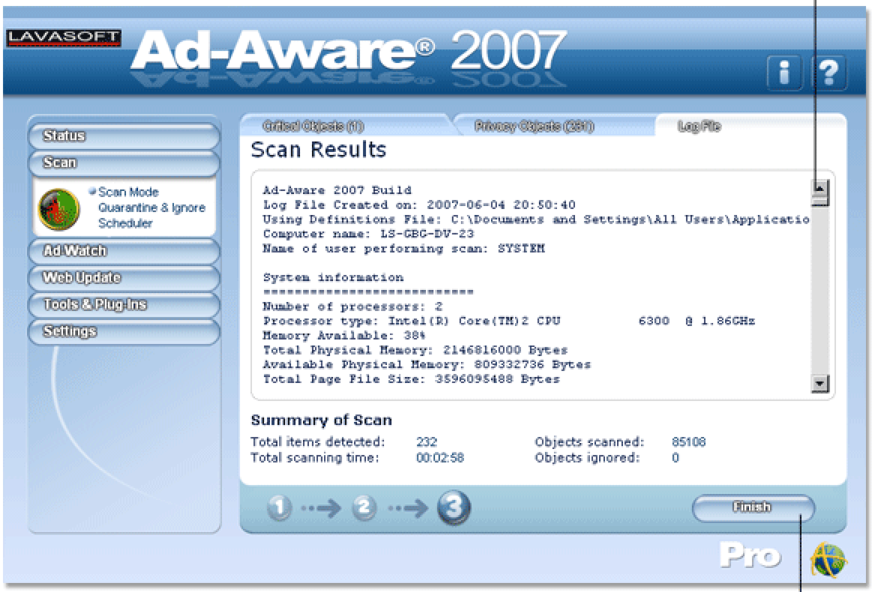
Click to select all objects detected in this category.

For each detected privacy object, you can choose to add it to the Ignore List or remove it from your system by checking the box beside the object(s) and then clicking one of these buttons.

Log File

The log file contains information about the scan; it is a record of the action that occurred during the scan. You can adjust the amount and type of information contained in the log file in the Ad-Aware 2007 settings.

Scroll down to view the details of your log file.



Scan Results

```
Ad-Aware 2007 Build
Log File Created on: 2007-06-04 20:50:40
Using Definitions File: C:\Documents and Settings\All Users\Applicatio
Computer name: LS-GBG-DV-23
Name of user performing scan: SYSTEM

System information
===========================
Number of processors: 2
Processor type: Intel(R) Core(TM)2 CPU          6300  @ 1.86GHz
Memory Available: 38%
Total Physical Memory: 2146816000 Bytes
Available Physical Memory: 809332736 Bytes
Total Page File Size: 3596095488 Bytes
```

Summary of Scan

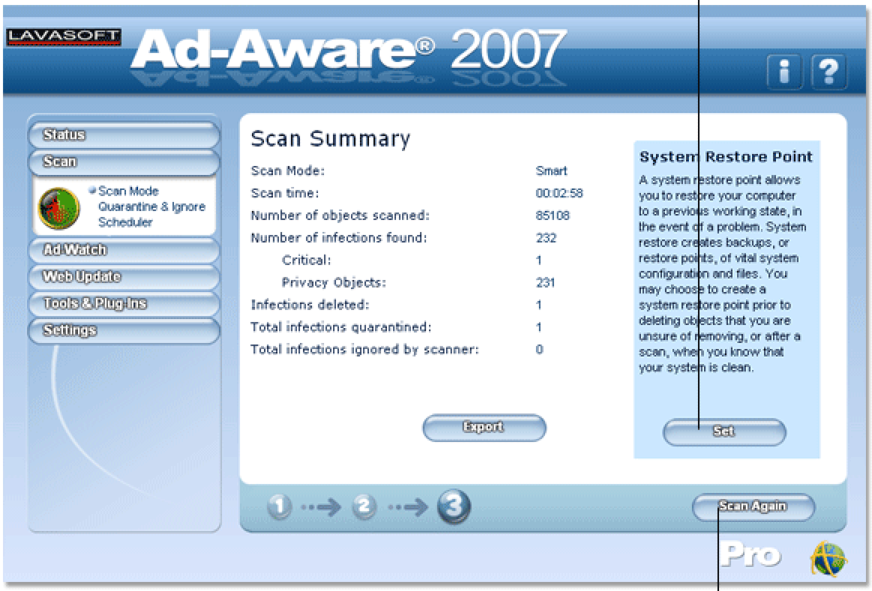
Total items detected:	232	Objects scanned:	85108
Total scanning time:	00:02:58	Objects ignored:	0

Click to go to the Scan Summary screen.

Scan Summary

The "Scan Summary" screen shows information about the scan that you performed and the number of objects that were detected, deleted, ignored by the scanner, and quarantined.

Click to create a system restore point, when you know that your system is clean.



Scan Summary

Scan Mode:	Smart
Scan time:	00:02:58
Number of objects scanned:	85108
Number of infections found:	232
Critical:	1
Privacy Objects:	231
Infections deleted:	1
Total infections quarantined:	1
Total infections ignored by scanner:	0

System Restore Point

A system restore point allows you to restore your computer to a previous working state, in the event of a problem. System restore creates backups, or restore points, of vital system configuration and files. You may choose to create a system restore point prior to deleting objects that you are unsure of removing, or after a scan, when you know that your system is clean.

Click to re-scan your system, or use the main menu to navigate to another part of Ad-Aware 2007.

Quarantine

Quarantine is used to isolate and backup objects detected during an Ad-Aware 2007 scan. You then have the option to restore them at a later time. Objects that are quarantined will be encrypted and compressed, and can only be read and restored using the Ad-Aware 2007 Quarantine manager. Objects stored in Quarantine do not pose a threat to your computer.

The Quarantine manager lists objects by:

- Family: Shows the family associated with the detected objects.
- Category: Shows the category that Lavasoft has classified that threat to be in.
- Description: Shows a description of the object's location.
- TAI: Shows the Threat Analysis Index (TAI) of the detected object.
- Time: Shows the date and time you quarantined the object.

Add Objects to Quarantine

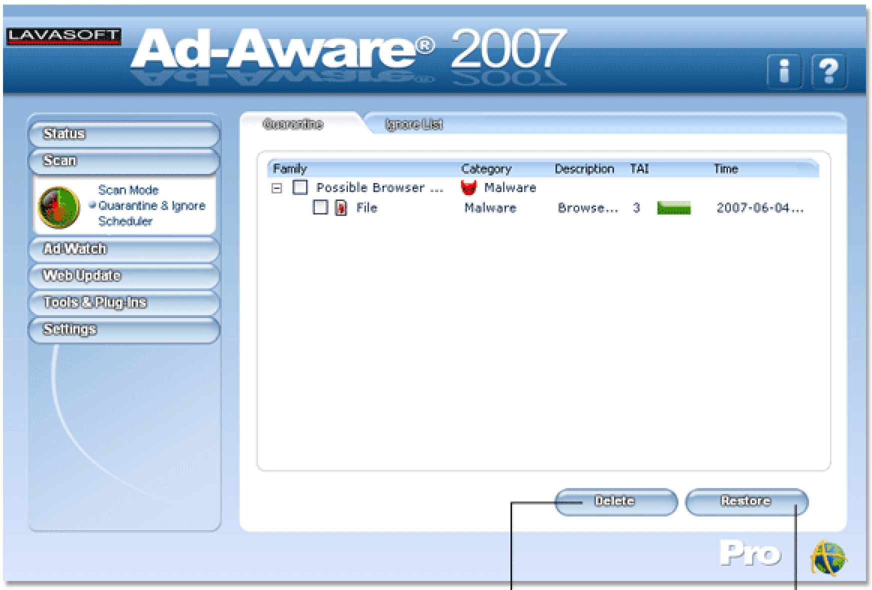
To add an object to Quarantine, you must first run an Ad-Aware 2007 scan. From the Scan Results screen, select the object or objects you would like to Quarantine by checking the box beside it. Click the "Quarantine" button to quarantine the object or objects. You can then open the Quarantine manager to see a list of quarantined objects.

Restore Quarantined Objects

In the Quarantine manager, select the quarantined object or objects you would like to restore by checking the box beside it. When you click "Restore," the object/objects will be removed from Quarantine.

Automatic Quarantine

You can set Ad-Aware 2007 to automatically quarantine objects prior to removal. Click the "Settings" button and select the "Auto Scans" tab. Under "Safety," check the button next to "Quarantine objects prior to removal."



Family	Category	Description	TAI	Time
⊟ ☐ Possible Browser ...	Malware			
☐ File	Malware	Browse...	3 🟩	2007-06-04...

Select an object and click to remove it from your system.

Select an object and click to remove it from Quarantine.

Ignore List

The Ignore List can be used when you want to keep a particular detected item installed on your system, and do not want Ad-Aware 2007 to remove it. When you add items to the Ignore List, Ad-Aware 2007 will not detect them when your system is scanned.

The Ignore List lists types of objects together by category, and shows a description of each object's location.

Add Objects to Ignore List

To add an object to the Ignore List, you must first run an Ad-Aware 2007 scan. From the Scan Results screen, select the object or objects you would like to add to the Ignore List by checking the box beside it. Click the "Add to Ignore" button and the object/objects will be added to the Ignore List.

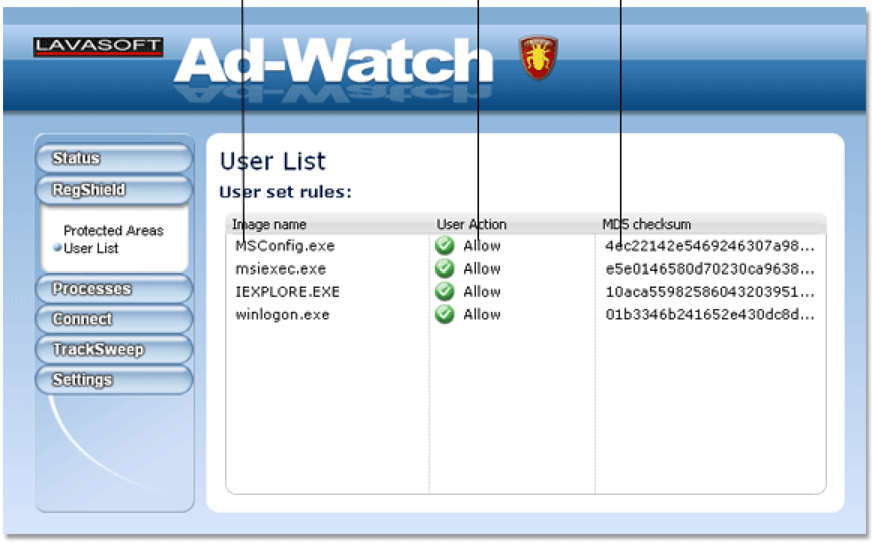
Remove Objects from Ignore List

After accessing the Ignore List, select the object or objects you would like to remove from the Ignore List by checking the box beside it. Click "Delete" to remove the selected object/objects from the Ignore List.

Names of applications that have attempted to make changes to the registry.

Click the checkmark to set the registry access rights for each application to either 'Allow', 'Block' or 'not set', which will prompt the user for every change.

The MD5 checksum is a unique identifier for each application.



User List

User set rules:

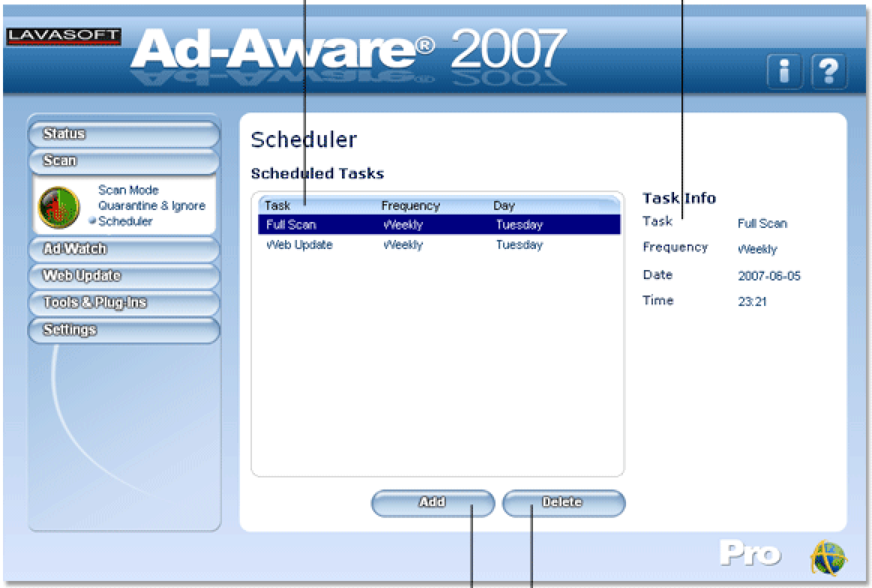
Image name	User Action	MD5 checksum
MSConfig.exe	✓ Allow	4ec22142e5469246307a98...
msiexec.exe	✓ Allow	e5e0146580d70230ca9638...
IEXPLORE.EXE	✓ Allow	10aca55982586043203951...
winlogon.exe	✓ Allow	01b3346b241652e430dc8d...

Scheduler Plus Pro

Click "Scheduler" from the drop-down "Scan" menu to open the Ad-Aware 2007 Scheduler. You can use the Scheduler to automatically perform Web Updates and automatically scan your computer on specific dates, at set times.

Shows all of the scans and Web Updates that you have scheduled for Ad-Aware 2007 to perform.

When you select a task in the Scheduler, more information is shown here about that specific task.



Scheduler

Scheduled Tasks

Task	Frequency	Day
Full Scan	Weekly	Tuesday
Web Update	Weekly	Tuesday

Task Info

Task	Full Scan
Frequency	Weekly
Date	2007-06-05
Time	23:21

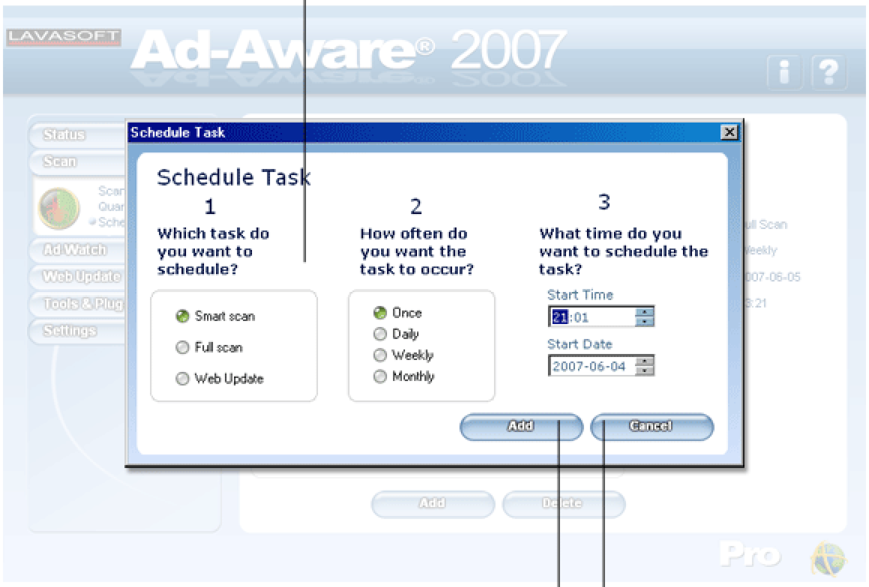
Click to schedule scans or Definitions File updates.

Select a task and click to remove it from the Scheduler.

Schedule Task

To schedule a task, click "Add" and follow the steps in the "Schedule Task" window to schedule the type of task to perform, its frequency, and the date/time you want it to start.

Follow the three steps and then click "Add" to schedule the task.



Schedule Task

1 Which task do you want to schedule?

● Smart scan
○ Full scan
○ Web Update

2 How often do you want the task to occur?

● Once
○ Daily
○ Weekly
○ Monthly

3 What time do you want to schedule the task?

Start Time: 21:01

Start Date: 2007-06-04

Click to schedule the task.

Click to cancel the task and return to the Scheduled Task screen.

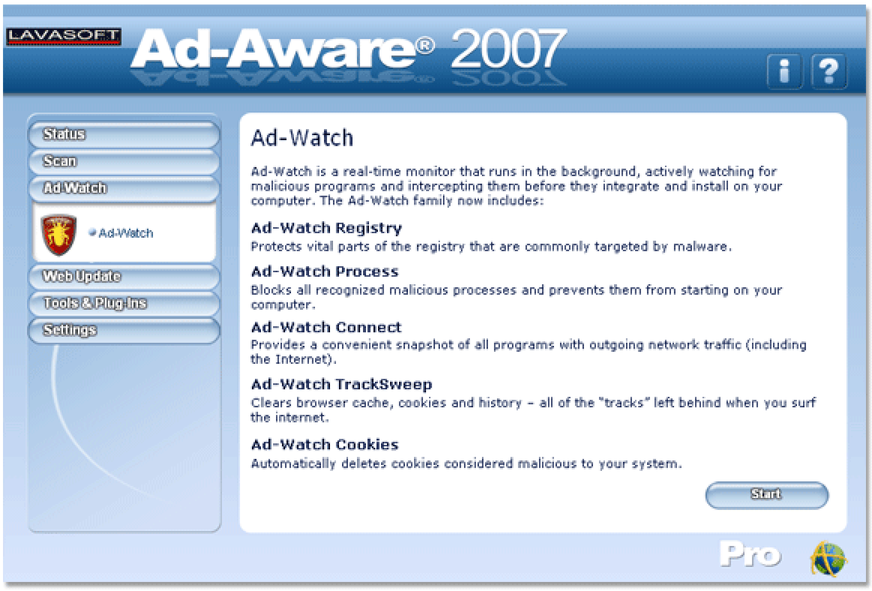
A message will appear in the notification area of your taskbar when a scheduled Web Update is taking place.

The Ad-Aware 2007 icon in the notification area of your taskbar will begin to blink, and a message will appear to let you know when a scheduled scan has begun and finished. To stop a scheduled scan that is in progress, you can right-click on the Ad-Aware 2007 icon in the system tray and select "Stop Scan."

Note! If your computer is not turned on at the date and time a task is scheduled to occur, the task will not occur until the next scheduled time.

Ad-Watch Plus Pro

After clicking "Ad-Watch" on the Ad-Aware 2007 main menu, launch the program by clicking "Start".



Ad-Watch

Ad-Watch is a real-time monitor that runs in the background, actively watching for malicious programs and intercepting them before they integrate and install on your computer. The Ad-Watch family now includes:

Ad-Watch Registry
Protects vital parts of the registry that are commonly targeted by malware.

Ad-Watch Process
Blocks all recognized malicious processes and prevents them from starting on your computer.

Ad-Watch Connect
Provides a convenient snapshot of all programs with outgoing network traffic (including the Internet).

Ad-Watch TrackSweep
Clears browser cache, cookies and history - all of the "tracks" left behind when you surf the internet.

Ad-Watch Cookies
Automatically deletes cookies considered malicious to your system.

The Ad-Watch module will open, displaying the main menu screen.

Ad-Watch is the real-time monitor featured in both Ad-Aware 2007 Plus and Ad-Aware 2007 Pro. The scanner in Ad-Aware 2007 detects and cleans malware from your system, but Ad-Watch goes a step further. From the moment your machine is turned on, Ad-Watch is watching, actually catching these programs before they integrate and install on your PC. If malware or parasites are detected, an Ad-Watch notification window will appear in the notification area of your taskbar, giving you the choice to allow or block that particular process or registry change or addition.

Ad-Watch allows you to lock the start-up sections of your registry, block possible and actual browser hijack attempts, block suspicious processes, lock executable file associations, and block malicious cookies.

Because Ad-Watch uses the same Definitions File as Ad-Aware, it is important to get updates regularly from Lavasoft's Detection Database.

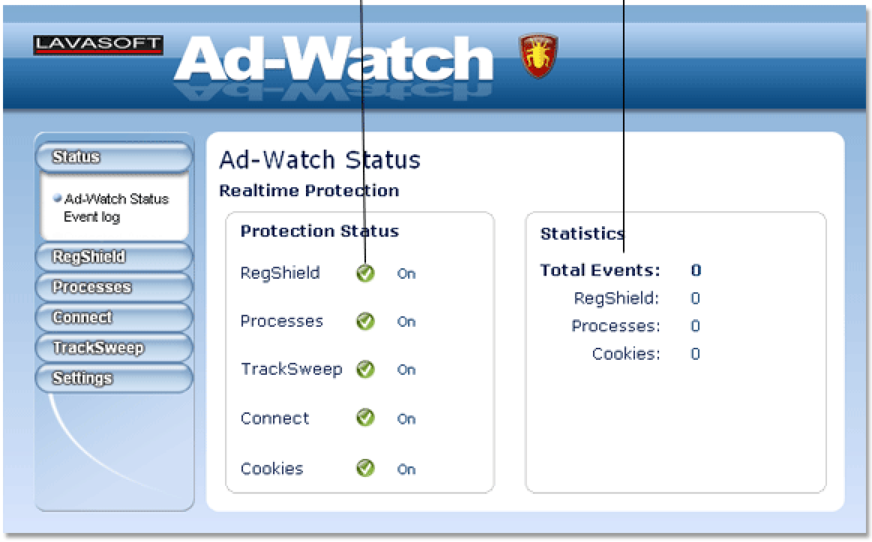
Ad-Watch has been re-designed and now features four different protection tools: RegShield, Processes, Connect, and TrackSweep. Similar to the Ad-Aware 2007 interface, Ad-Watch also has a "Settings" screen where you can make specific changes to the actions that Ad-Watch performs.

Ad-Watch Status

The Ad-Watch "Status" screen gives you an overview of the Ad-Watch real-time monitor, allows you to activate the tools it consists of, and shows statistics from events you have been alerted about.

Select the buttons next to each of Ad-Watch's tools to turn them on or off.

Shows statistics on the events that Ad-Watch has detected.



Ad-Watch Status

Realtime Protection

Protection Status

RegShield	✓	On
Processes	✓	On
TrackSweep	✓	On
Connect	✓	On
Cookies	✓	On

Statistics

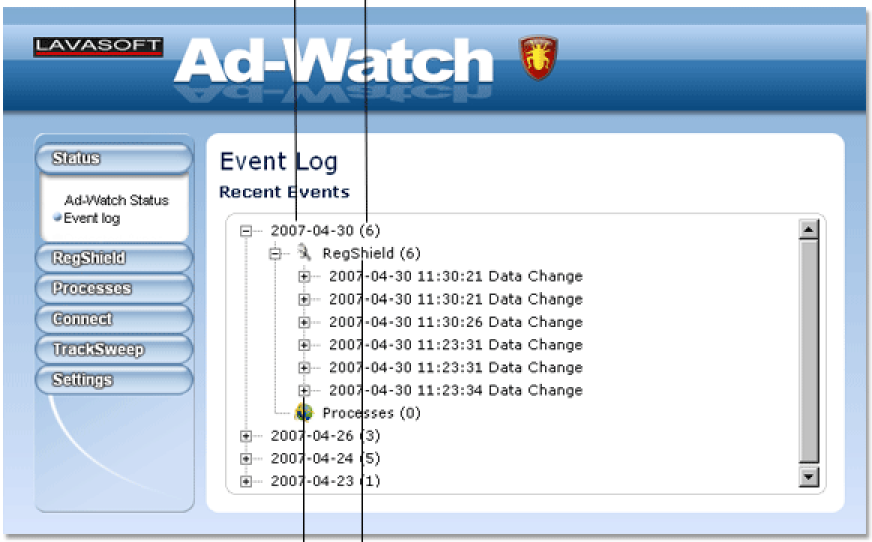
Total Events:	0
RegShield:	0
Processes:	0
Cookies:	0

Event Log

Ad-Watch's "Event Log" shows a list of all of the events detected by Ad-Watch, such as blocked processes, blocked registry changes or cleaning events (items cleaned by TrackSweep).

Events are listed according to the date they occurred. The most recent events are shown at the top of the log.

Shows the number of events detected on that day.



Event Log

Recent Events

```
⊟ 2007-04-30 (6)
   ⊟ RegShield (6)
      ⊞ 2007-04-30 11:30:21 Data Change
      ⊞ 2007-04-30 11:30:21 Data Change
      ⊞ 2007-04-30 11:30:26 Data Change
      ⊞ 2007-04-30 11:23:31 Data Change
      ⊞ 2007-04-30 11:23:31 Data Change
      ⊞ 2007-04-30 11:23:34 Data Change
     Processes (0)
⊞ 2007-04-26 (3)
⊞ 2007-04-24 (5)
⊞ 2007-04-23 (1)
```

Click to expand the log to see more detailed information.

Events are listed according to their specific type.

Ad-Watch RegShield Plus Pro

Select "RegShield" in the Ad-Watch main menu to open the RegShield screen.

The registry is a database that stores settings and options for the operating system for Microsoft Windows 32-bit and 64-bit versions. The registry contains information and settings for the hardware, operating system software, users, and preferences of your computer.

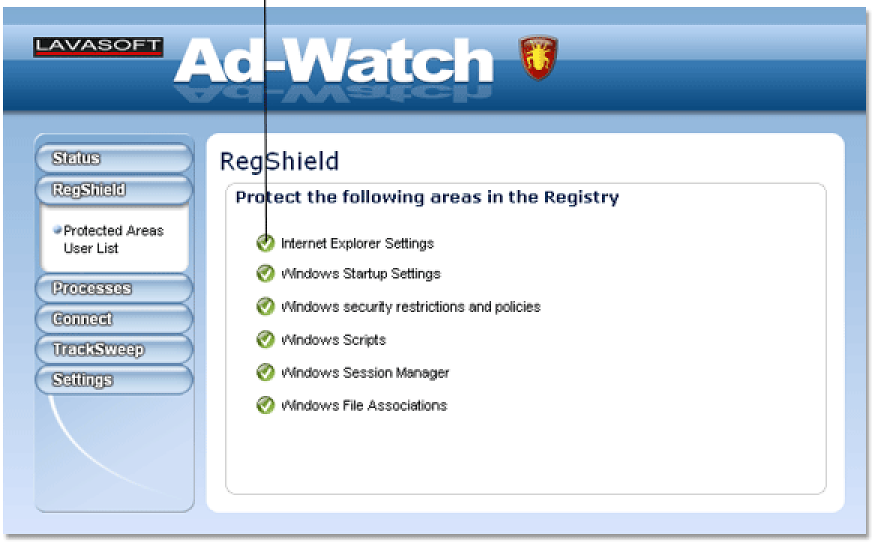
RegShield allows you to protect the areas in your registry that are common targets for malware by alerting you when a program attempts to make changes to sections in your registry.

Protected Areas

RegShield allows you to protect the following areas of your registry:

- Internet Explorer Settings: Internet Explorer stores settings in the registry that contain information on your default home page and default search page, as well as other user settings that control the browser's behavior. These settings are common targets for browser hijackers.
- Windows Start-up Settings: Windows start-up settings affect which parts of Windows are loaded at start-up and what programs are started.
- Windows security Restrictions and Policies: These are settings for user access rights, and other security settings that are used to protect the system's integrity by making it harder to change files and folders that are vital for Windows to run properly.
- Windows Scripts: Windows Scripts are executed when logging-in to Windows.
- Windows Session Manager: Session Manager keeps track of your current system state, including the applications that are open and the documents each application has opened, so that the same state can be restored when you log-in or log-out.
- Windows File Associations: This data is needed to associate certain file types with certain programs (for example, to associate ".psd" with Photoshop, or ".html" with your browser of choice).

Check the button next to each area of the registry that you want RegShield to protect.



RegShield

Protect the following areas in the Registry

✓ Internet Explorer Settings
✓ Windows Startup Settings
✓ Windows security restrictions and policies
✓ Windows Scripts
✓ Windows Session Manager
✓ Windows File Associations

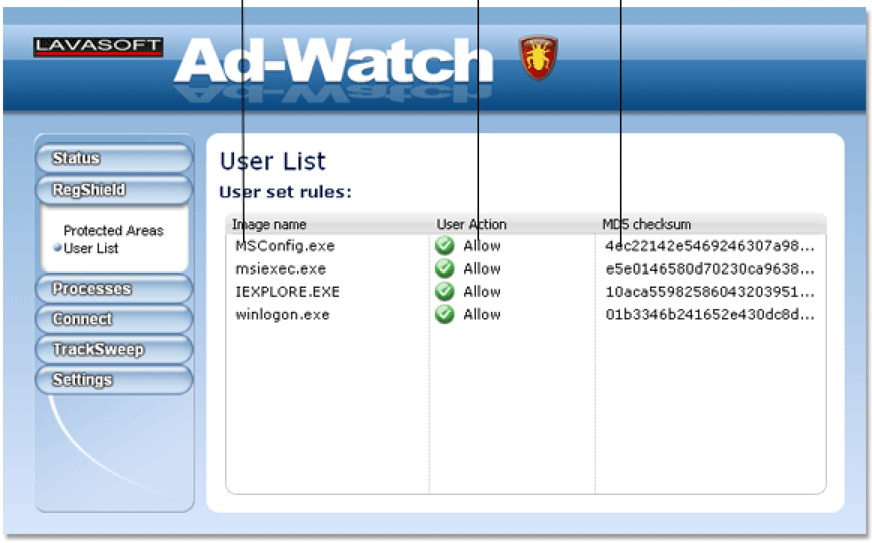
User List

The user list lets you control the access rights to the registry on an application basis. You

Names of applications that have attempted to make changes to the registry.

Click the checkmark to set the registry access rights for each application to either 'Allow', 'Block' or 'not set', which will prompt the user for every change.

The MD'5 checksum is a unique identifier for each application.



User List

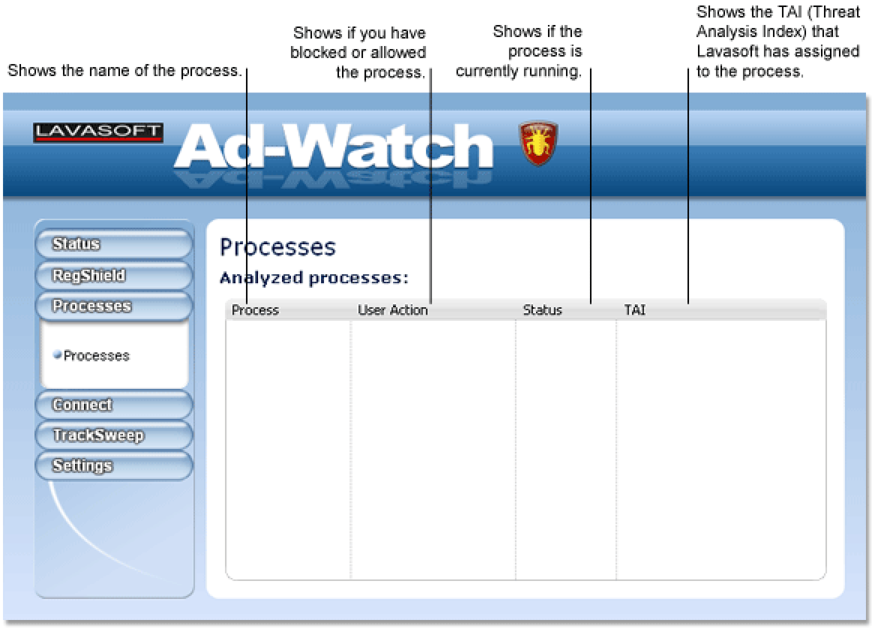
User set rules:

Image name	User Action	MD5 checksum
MSConfig.exe	✓ Allow	4ec22142e5469246307a98...
msiexec.exe	✓ Allow	e5e0146580d70230ca9638...
IEXPLORE.EXE	✓ Allow	10aca55982586043203951...
winlogon.exe	✓ Allow	01b3346b241652e430dc8d...

Ad-Watch Processes Plus Pro

Select "Processes" in Ad-Watch's main menu to open the Ad-Watch Processes screen.

The Processes screen displays the processes that you have been alerted about by Ad-Watch because they are in detection in the Lavasoft Detection Database. Each process is show with its corresponding TAI (Threat Analysis Index) rate so you can easily assess its threat level. You can choose to remove analyzed processes from the list of processes, block any processes that you had previously chosen to allow, and allow any processes that you had previously chosen to block.

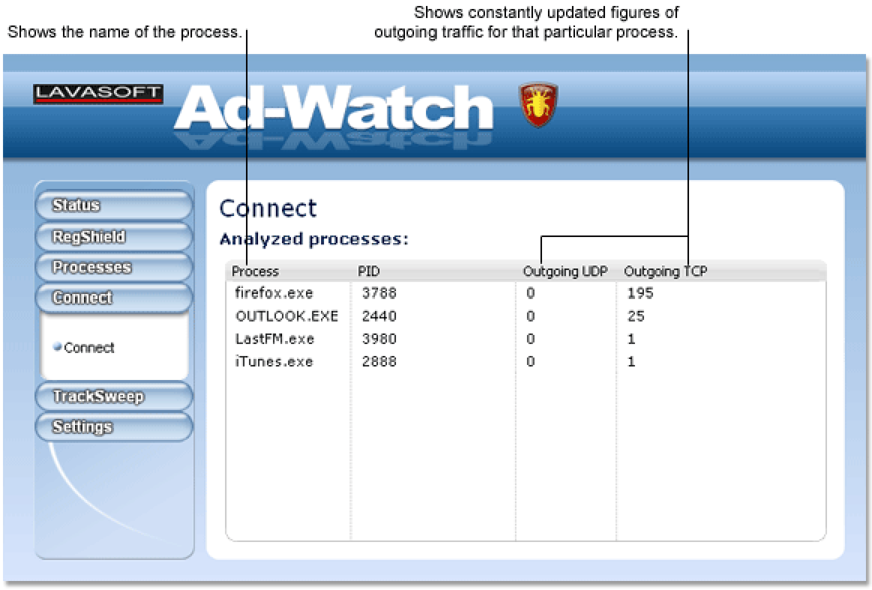

Shows the name of the process.
Shows if you have blocked or allowed the process.
Shows if the process is currently running.
Shows the TAI (Threat Analysis Index) that Lavasoft has assigned to the process.
LAVASOFT
Ad-Watch
Status
RegShield
Processes
Processes
Connect
TrackSweep
Settings
Processes
Analyzed processes:
Process
User Action
Status
TAI

Ad-Watch Connect Pro

Select "Connect" in the Ad-Watch main menu to open the Ad-Watch Connect screen.

Ad-Watch Connect allows you to monitor network traffic, so that you are able to examine network statistics for all running processes.

The Ad-Watch Connect screen shows a list of all running processes, and allows you to see detailed network information on each process. If the process is in detection, its TAI (Threat Analysis Index) rate will be shown, so you can easily assess its threat level.


Shows the name of the process.
Shows constantly updated figures of outgoing traffic for that particular process.
LAVASOFT
Ad-Watch
Status
RegShield
Processes
Connect
Connect
TrackSweep
Settings

Connect

Analyzed processes:

Process	PID	Outgoing UDP	Outgoing TCP
firefox.exe	3786	0	195
OUTLOOK.EXE	2440	0	25
LastFM.exe	3980	0	1
iTunes.exe	2888	0	1

Connect Context Menu

Right-click on a process and choose "Traffic Details," to open the Traffic Details window, which shows you detailed information on that particular process.

Ad-Watch TrackSweep Plus Pro

Select "TrackSweep" in the Ad-Watch main menu to open the TrackSweep screen.

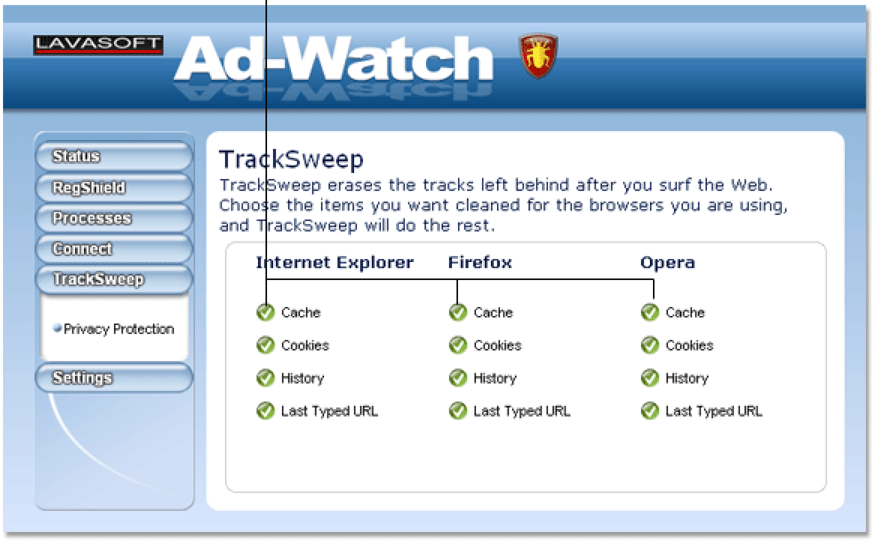
TrackSweep is a privacy tool that allows you to remove the traces of your Internet browsing from your system.

By checking the buttons next to the items of your choice, the tracks left behind when you surf the Internet can be cleaned from Internet Explorer, Firefox, and Opera web browsers whenever you close a web browser.

You can choose to clean the following areas:

- Cache: Clears your browser cache, or Temporary Internet Files.
- Cookies: Clears browser cookies – data that a website saves on your computer's hard drive and retrieves when you revisit the site.
- History: Clears your full history of visited websites.
- Last typed URLs: Clears the list of last accessed URL's from your web browser's address bar.
- Browser tabs: If you use tabbed browsing, your browser tabs will be cleared.

Choose the browser items you want TrackSweep to clean from your choice of web browsers by checking the box next to each item.



TrackSweep

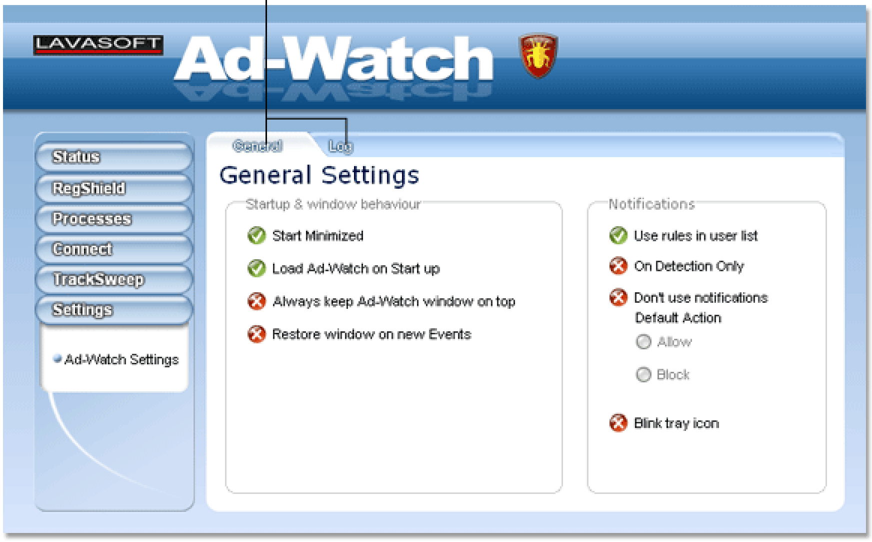
TrackSweep erases the tracks left behind after you surf the Web. Choose the items you want cleaned for the browsers you are using, and TrackSweep will do the rest.

Internet Explorer	Firefox	Opera
☑ Cache	☑ Cache	☑ Cache
☑ Cookies	☑ Cookies	☑ Cookies
☑ History	☑ History	☑ History
☑ Last Typed URL	☑ Last Typed URL	☑ Last Typed URL

Ad-Watch Settings

Select "Settings" in the Ad-Watch main menu to open the settings screen to adjust Ad-Watch to better suit your individualized specifications.

Use the tabs at the top of the screen to navigate between different categories of settings.



General Settings

Startup & window behaviour

- ✓ Start Minimized
- ✓ Load Ad-Watch on Start up
- ✗ Always keep Ad-Watch window on top
- ✗ Restore window on new Events

Notifications

- ✓ Use rules in user list
- ✗ On Detection Only
- ✗ Don't use notifications

Default Action

- ○ Allow
- ○ Block

- ✗ Blink tray icon

Below is a description of the different settings that you can select in each category. Check the button next to each setting you would like to implement.

General

Ad-Watch

- Load Ad-Watch on start-up: If activated, Ad-Watch will start with Windows.
- Start minimized: Ad-Watch icon will show in your taskbar.
- Always keep Ad-Watch window on top: This option will force the Ad-Watch window to stay on top of all other open windows.
- Restore window on new events: This will cause the Ad-Watch window to open only when a new event has been detected.

Notifications

- On detection only: Notification messages will only appear on detection of events.
- Do not use notifications: Notification messages will not be used. Select either allow or block as the default action.

Log

By default, Ad-Watch logs all events in the Event Log. You may choose to change the event log options for Registry Events, Process Events, TrackSweep Events, and Cookies Events. Check the button next to the events that you want Ad-Watch to log.

Web-Update

Click "Web Update" on the main menu and select "Web Update" from the drop-down menu to open the Web Update screen.

Web Update allows you to connect directly to the Lavasoft Security Center to look for Definitions File and software updates for Ad-Aware 2007. To stay protected from the latest threats, it is important to run regular Web Updates, to have the most recent Definitions File update from the Lavasoft Detection Database. You can also receive software version updates through Web Update as they become available.

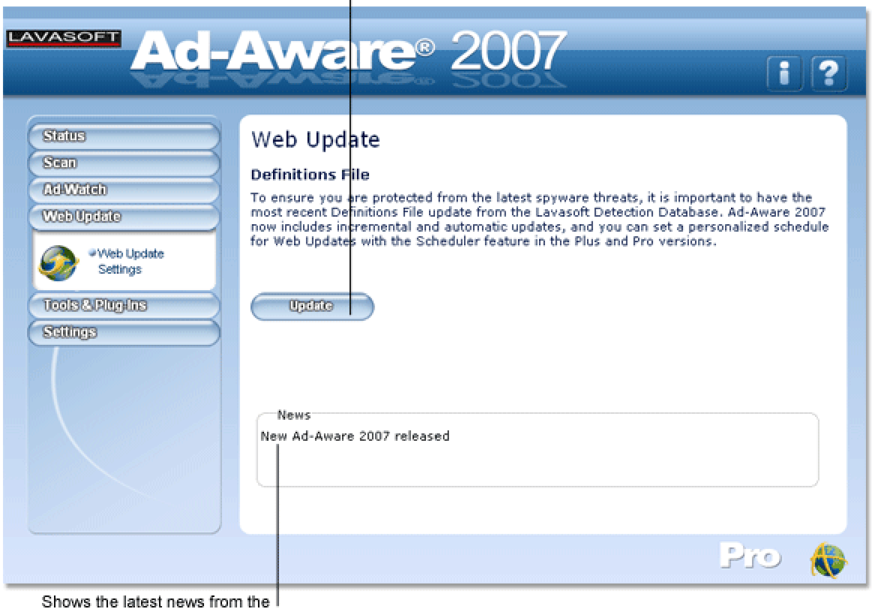
The Detection Database is Ad-Aware 2007's extensive threat detection list, and allows Ad-Aware 2007 to detect the latest threats on your system. When you update the Detection Database with the latest Definitions File, you download an incremental update from the database, guaranteeing you a quick, easy update. The file will automatically be stored in the correct location on your computer

Update Ad-Aware 2007

While you can get the latest Definitions File by performing a manual update, Web Update is a simple way to update the Detection Database. When you perform a Web Update, you will receive verification that your Definitions File is up-to-date or you will be prompted to confirm that you want to download the latest file. The update manager will then launch if there is a new software version available, allowing you to choose to update the software.

You can also use the Scheduler to set up automatic Web Updates to occur at specific dates and times, and change the Ad-Aware 2007 settings so that an automatic Web Update is performed prior to scans.

Click to check if new Definitions File and software updates are available.



Web Update

Definitions File

To ensure you are protected from the latest spyware threats, it is important to have the most recent Definitions File update from the Lavasoft Detection Database. Ad-Aware 2007 now includes incremental and automatic updates, and you can set a personalized schedule for Web Updates with the Scheduler feature in the Plus and Pro versions.

New Ad-Aware 2007 released

Shows the latest news from the Lavasoft Security Center.

Web-Update Settings

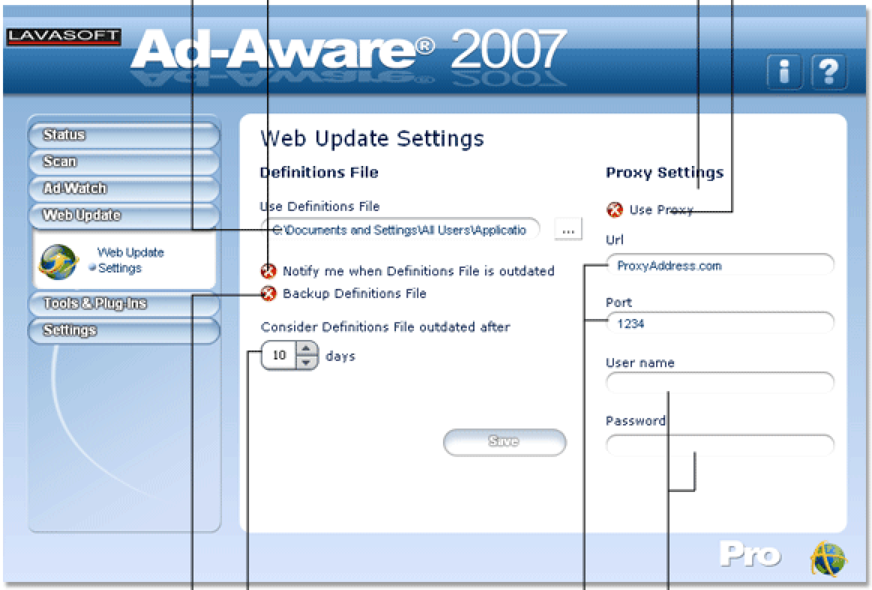
Select "Settings" from the Web Update drop-down menu to change the Definitions File and Proxy settings.

Shows the name and location of where the Definitions File is stored.

A notification window will appear when you start Ad-Aware 2007, if the Definition File is outdated.

will need to have your proxy settings correctly configured in order to perform a Web Update.

Turns the proxy settings on or off.



Web Update Settings

Definitions File

Use Definitions File: C:\Documents and Settings\All Users\Applicatio ...

☒ Notify me when Definitions File is outdated

☒ Backup Definitions File

Consider Definitions File outdated after 10 days

Save

Proxy Settings

☒ Use Proxy

Url: ProxyAddress.com

Port: 1234

User name

Password

Creates a backup of the current Definitions File before downloading and installing a new one.

Sets a timeframe to remind you when the Definitions File is outdated.

Enter the IP address and the port that your proxy uses

Enter your network log-in information.

Automatic Web Update

You can use the Scheduler to schedule automatic Web Updates to occur at set times. To open the Scheduler, click the "Scan" menu button and then click "Scheduler" in the drop-down menu. Click "Add," select "Web Update" from the list of tasks, and then specify the frequency, date and time for the Web Update to occur.

You can also adjust the Ad-Aware 2007 settings to automatically update the Detection Database prior to scanning your computer. Click the "Settings" button to open Ad-Aware 2007's settings menu. Select the "Auto Scans" tab. Under "System," check the box next to "Update Definitions File before scanning." If an updated file is available, it will automatically be downloaded to your computer before scanning. Click "Save" to save your changes.

Manual Update

In some circumstances, such as if your proxy settings are not configured properly, you may not be able to update the Detection Database by using Web Update. You can manually update the Detection Database with the latest Definitions File by following the steps below.

- Close Ad-Aware 2007.
- Download the latest Definitions File in a ZIP file from the Lavasoft website.
- Save the file to a temporary location.
- When complete, unzip the contents of the file to the installation directory of Ad-Aware 2007, which is usually C:\Program Files\Lavasoft\Ad-Aware 2007\.
- Open Ad-Aware 2007. You can confirm the latest Definitions File is installed by looking at "Update Status" on Ad-Aware 2007's main status screen.

Tools & Plug-ins

Click the "Tools & Plug-ins" menu button to open the "Tools & Plug-ins" drop-down menu. Click "Tools" to open the Process Watch and Hosts File Editor menu screen. Click "Start" to launch Process Watch or Hosts File Editor. Process Watch and Hosts File Editor are both stand-alone tools, and their modules will be launched separately from the Ad-Aware 2007 user interface.

Process Watch Plus Pro

Process Watch is a powerful process viewer and manager. It is a stand-alone tool that allows you to browse and terminate running processes and their associated modules.

Process Watch allows you to view detailed information on all processes that are running on your system to see if there are any known offending processes. By default, Process Watch lists all processes that are connected to visible windows on your desktop. You can then choose to quickly terminate any running process or unload a module, if necessary.

Note! Be careful; some processes and modules are needed by Windows or other software in order to function.

Using Process Watch

When the Process Watch module is launched, it shows you a snapshot of all the running processes (top window), their associated modules (lower left window), and a list of threads running for current processes (lower right window). This snapshot is constantly refreshed, and your screen is automatically updated.

The Process Watch displays three main lists of information. The upper list is the process window, displaying the processes that are currently running in your system. In order to see a more in-depth picture of where each process originated, the module shows a "graphic tree"; the parent process tops each "graphic tree," and branches down to show the spawned sub-processes. The lower left list is the module window, showing a list of the modules the selected process has loaded into memory. The lower right list is the thread window, showing a module's thread, or path of execution.

Process Window

The top window of the Process Watch module is the process window. The columns of specific information on each process are listed below.

Processes are briefly color-coded as an action occurs, to give you quick, additional information. When a process is highlighted green, it indicates that the process has recently started. A process will be highlighted yellow when suspended, and will remain yellow until you choose to resume it. A process is highlighted red when it has been terminated.

The process window lists information by:

- Process: Lists the file name of all processes running in your system.
- PID: Shows the process ID – a unique identifier for each process.
- CPU: Shows the percentage of CPU time being used by a given process. (The Process Watch can support more than one process; these are taken into account, and you are given an accurate CPU percentage.)
- Memory: Shows the amount of memory used by the process.
- Threads: Shows the number of threads the process uses.
- Priority: Shows the operating system's assigned level of importance.
- Created: Shows a time stamp of when the process was created.
- Path: Shows where the operating system loaded the process into memory.

Process Window Context Menu

Right-clicking on a process in the top, main screen opens the process window context menu, showing the operations you can perform on any given process.

You can choose from the following operations:

- Terminate: Terminates the selected process.
- Terminate Tree: Terminates the selected parent process and all of its sub-processes.
- Restart: Starts the process again from the beginning.
- Suspend: Freezes a selected process, so that it temporarily stops running.
- Resume: Resumes the execution of a process that has been suspended.
- Set Priority: Manually change the priority level that was assigned by the operating system. The priority level can be reassigned to:
  - Real Time: Highest possible priority level; pre-empts all other processes, including operating system processes performing important tasks.
  - High: Piority level of time-critical tasks that must be executed immediately.
  - Above Normal*: Priority level above the normal level.
  - Normal: Piority level with no special scheduling needs.
  - Below Normal*: Priority level below the normal level.
  - Low: Priority level set to run the process when the system is idle.
- Open Folder: Opens the folder that contains the file spawning the selected process.
- Google: Brings you directly to a Google search to access more information about the selected process.
- Process Details: Opens the "Process Details" window which shows a graph of the estimated CPU usage of the process and more detailed information on that particular process. (You can also access Process Details by double-clicking on a process.)
- Columns: Allows you to add or remove any of the columns of information displayed in the process window.

Module Window

The lower left window of the Process Watch module is the module window. Click a process in the process window to have its details shown in the windows below.

The module window lists information by:

- Module: File name of the module.
- Base Address: Module's point of origin - where it started executing.
- Size: Allocated memory size for the selected module.
- Path: Full path of the module - where the module is located.

Module Window Context Menu

Right-clicking on a module in the module window opens the module window context menu, showing the operations you can perform on any given module.

You can choose from the following operations:

- Unload: Unloads the selected module from memory.
- Open Folder: Opens the folder that contains the file spawning the selected module.
- Google: Brings you directly to a Google search to access more information about the selected module.

Thread Window

The lower right window of the Process Watch module is the thread window. Click a process in the process window to have its details shown in the windows below.

The thread window lists information by:

- Thread: ID number assigned by the operating system - the thread's unique identifier.
- Priority: Priority level allocated by the operating system.

The process window shows the processes currently running in your system.

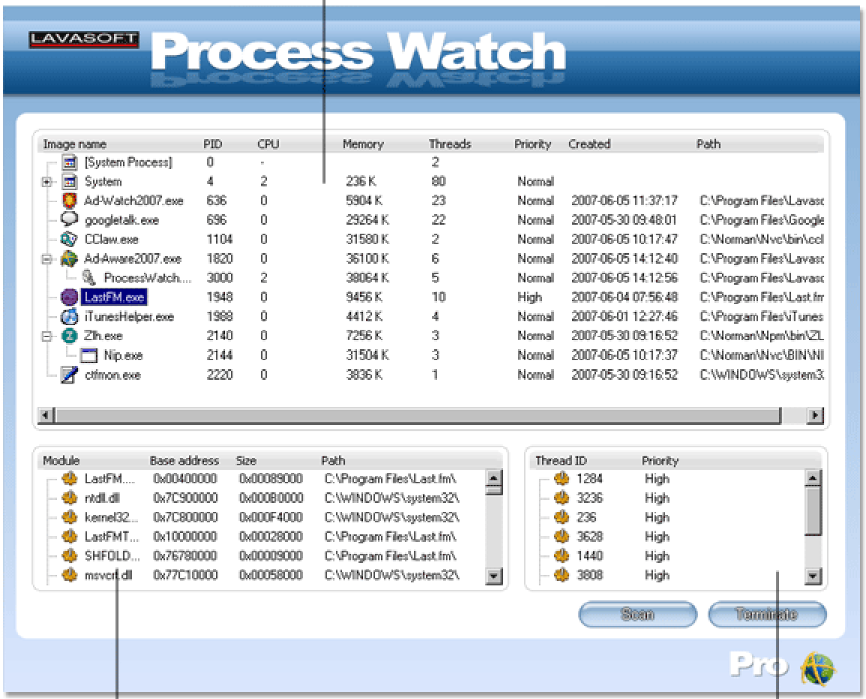


Image name	PID	CPU	Memory	Threads	Priority	Created	Path
[System Process]	0	-		2			
System	4	2	236 K	80	Normal		
Ad-Watch2007.exe	636	0	5904 K	23	Normal	2007-06-05 11:37:17	C:\Program Files\Lavasc
googletalk.exe	696	0	29264 K	22	Normal	2007-05-30 09:48:01	C:\Program Files\Google
CClaw.exe	1104	0	31580 K	2	Normal	2007-06-05 10:17:47	C:\Norman\Nvc\bin\ccl
Ad-Aware2007.exe	1820	0	36100 K	6	Normal	2007-06-05 14:12:40	C:\Program Files\Lavasc
ProcessWatch....	3000	2	38064 K	5	Normal	2007-06-05 14:12:56	C:\Program Files\Lavasc
LastFM.exe	1948	0	9456 K	10	High	2007-06-04 07:56:48	C:\Program Files\Last.fm
iTunesHelper.exe	1988	0	4412 K	4	Normal	2007-06-01 12:27:46	C:\Program Files\iTunes
Zlh.exe	2140	0	7256 K	3	Normal	2007-05-30 09:16:52	C:\Norman\Npm\bin\ZL
Nip.exe	2144	0	31504 K	3	Normal	2007-06-05 10:17:37	C:\Norman\Nvc\BIN\NI
ctfmon.exe	2220	0	3836 K	1	Normal	2007-05-30 09:16:52	C:\WINDOWS\system3

Module	Base address	Size	Path
LastFM....	0x00400000	0x00089000	C:\Program Files\Last.fm\
ntdll.dll	0x7C900000	0x00080000	C:\WINDOWS\system32\
kernel32...	0x7C800000	0x000F4000	C:\WINDOWS\system32\
LastFMT...	0x10000000	0x00028000	C:\Program Files\Last.fm\
SHFOLD...	0x76780000	0x00009000	C:\Program Files\Last.fm\
msvcrt.dll	0x77C10000	0x00058000	C:\WINDOWS\system32\

Thread ID	Priority
1284	High
3236	High
236	High
3628	High
1440	High
3808	High

The module window shows a list of the modules the selected process has loaded into memory.

The thread window shows a module's thread, or path of execution.

Hosts File Editor Plus Pro

The Hosts File Editor is a stand-alone tool that allows you to create navigation shortcuts, reverse browser hijack entries, block advertisement sites, assist with parental controls, and make other exceptions to normal Internet navigation.

Your Hosts File is used to associate host names with IP addresses. For example, the host name for Yahoo! is www.yahoo.com, while its IP address is 204.71.200.67. Both addresses will bring you to Yahoo!'s site, but the "www" address will first have to be translated into the IP address by your Hosts File.

Using Hosts File Editor

The Hosts File Editor allows you to make changes to normal Internet navigation by redirecting a host name to a different IP address.

Some spyware and malware attempt to change your Hosts File in order to redirect your browsing to another site. You can use the Hosts File editor to reverse browser hijack attempts, block advertisements sites, and redirect your Internet navigation.

Computers have a host address of their own, which is known as the "localhost" address. The localhost IP address is 127.0.0.1. If you type in a host name to the Hosts File Editor, and then redirect it to your localhost IP address, you have effectively blocked that host, since all attempts to access it will lead back to your localhost. Using this method, you can block sites that serve advertisements, sites that serve objectionable content, or any other site that you choose.

The Hosts File Editor lists your current Hosts File information by:

- Status: Shows if the entry is active or inactive. Changes to your Hosts File will only occur when the status of an entry is marked "ACTIVE."
- Hostname: Shows the URL that leads to the IP address of the entry.
- IP: Shows the IP address of the entry.
- Comment: Allows you to write in a brief comment of your own about that specific entry.

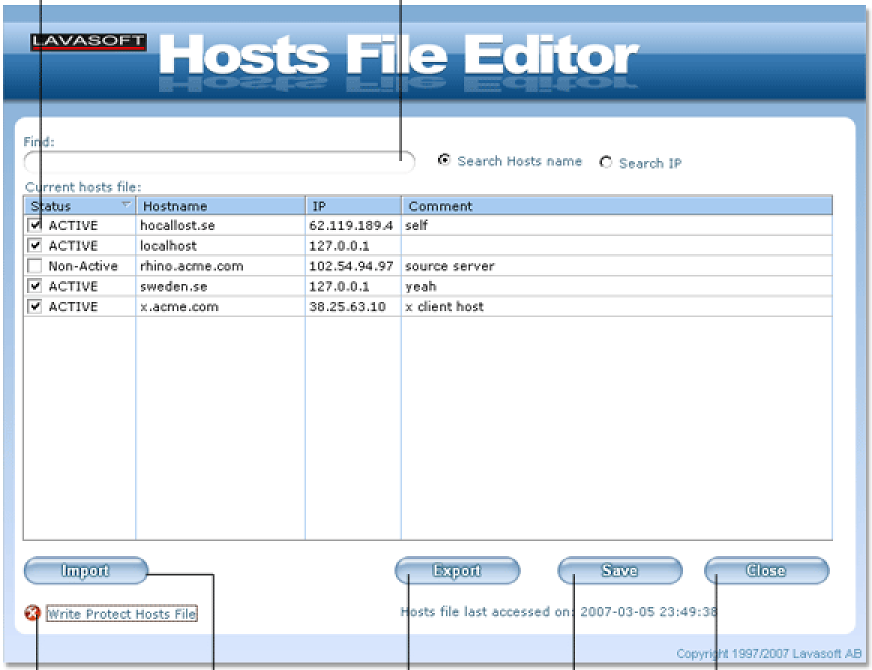
Hosts File Editor Context Menu

Right-click within the "Current Host File" screen to open the context menu where you can choose from the following operations:

- Add new entry: Add a new entry to your Hosts File. After you choose to add a new entry, a new entry will appear in "Current Hosts File" list. You can then double-click within the hostname, IP address or comments column in order to add that information.
- Delete entry: Delete a specific entry. Highlight an entry and then select "Delete entry" in order to delete that entry.
- Flush: Reset your Hosts File into a single localhost entry. If selected, all of your current entries will be deleted.

Check the box to change the status of the selected host name to active or inactive

Allows you to search through your current Host File for a specific IP address or Host name.



Find:

● Search Hosts name ○ Search IP

Current hosts file:

Status	Hostname	IP	Comment
☑ ACTIVE	hocallost.se	62.119.189.4	self
☑ ACTIVE	localhost	127.0.0.1	
□ Non-Active	rhino.acme.com	102.54.94.97	source server
☑ ACTIVE	sweden.se	127.0.0.1	yeah
☑ ACTIVE	x.acme.com	38.25.63.10	x client host

☒ Write Protect Hosts File

Hosts file last accessed on: 2007-03-05 23:49:38

Copyright 1997/2007 Lavasoft AB

Allows you to write-protect your Hosts File so that it cannot be altered by other programs.

Click to import other Hosts File entries into the Hosts File Editor.

Allows you to save your Hosts File as a text file.

Click to save the changes you made.

Click to close the Hosts File Editor.

Plug-ins

In the "Tools and Plug-ins" drop-down menu, click "Plug-ins" to access the plug-ins screen.

Plug-ins are extra software options that are designed to enhance and extend Ad-Aware 2007's protection. Plug-ins are not strictly necessary for Ad-Aware 2007 to perform its core purpose, but they can add an extra layer of defense against privacy and security intrusions.

Note! Ad-Aware SE plug-ins are not compatible with Ad-Aware 2007. As Ad-Aware 2007 plug-ins become available, you will be able to look for and download them from the Lavasoft Plug-ins and Tools page.

Using Plug-ins

Ad-Aware 2007 plug-ins are free, simple to download, and easy to use. To see more information on specific plug-ins and to download them, visit the Plug-ins and Tools page on Lavasoft's website and follow the installation instructions.

You can access the plug-ins you have installed by clicking "Plug-ins" in the "Tools & Plug-ins" drop-down menu.

Uninstalling Plug-ins

All plug-ins installed on your computer will be removed if you uninstall Ad-Aware 2007.

To uninstall a plug-in without removing Ad-Aware 2007:

Close Ad-Aware 2007

Click the Windows "Start" button.

Go to "Control Panel"

- Click "Add/Remove Programs"
- Locate the plug-in you wish to remove
- Click "Change/remove"
- Click "Next"
- Click "Finish" The plug-in is now removed.

TrackSweep

Select "TrackSweep" from the Tools and Plug-ins drop-down menu to access TrackSweep.

Ad-Aware 2007's TrackSweep feature is a privacy tool that allows you to remove all traces of your Internet browsing from your system.

By checking the buttons next to the items of your choice, and clicking "Clean", the tracks left behind when you surf the Internet can be cleaned from Internet Explorer, Firefox, and Opera web browsers. All browsers that are not running will be cleaned.

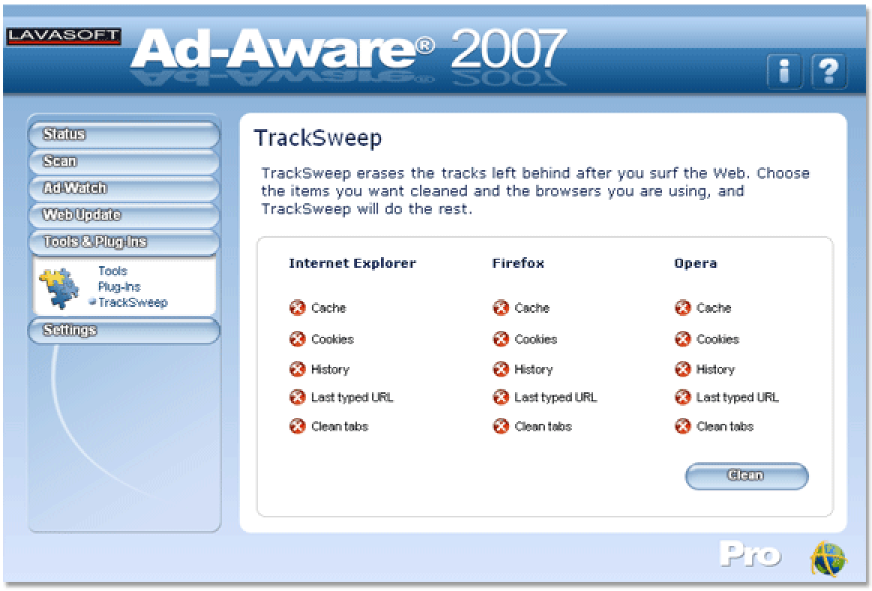
You can choose to clean the following areas:

- Cache: Clears your browser cache, or Temporary Internet Files.
- Cookies: Clears browser cookies – data that a website saves on your computer's hard drive and retrieves when you revisit the site.
- History: Clears your full history of visited websites.
- Last typed URLs: Clears the list of last accessed URL's from your web browser's address bar.
- Browser tabs: If you use tabbed browsing, your browser tabs will be cleared.

TrackSweep Context Menu

Right-click within TrackSweep's selection screen to open the context menu where you can choose from the following operations:

- Check all: Marks all items to be cleaned from every browser.
- Uncheck all: De-selects all items from being cleaned.
- Check all Explorer: Marks all Internet Explorer items to be cleaned.
- Uncheck all Explorer: De-selects all Internet Explorer items from being cleaned.
- Check all Firefox: Marks all Firefox items to be cleaned.
- Uncheck all Firefox: De-selects all Firefox items from being cleaned.
- Check all Opera: Marks all Internet Explorer items to be cleaned.
- Uncheck all Opera: De-selects all Internet Explorer items from being cleaned.



TrackSweep

TrackSweep erases the tracks left behind after you surf the Web. Choose the items you want cleaned and the browsers you are using, and TrackSweep will do the rest.

Internet Explorer	Firefox	Opera
☒ Cache	☒ Cache	☒ Cache
☒ Cookies	☒ Cookies	☒ Cookies
☒ History	☒ History	☒ History
☒ Last typed URL	☒ Last typed URL	☒ Last typed URL
☒ Clean tabs	☒ Clean tabs	☒ Clean tabs

Settings

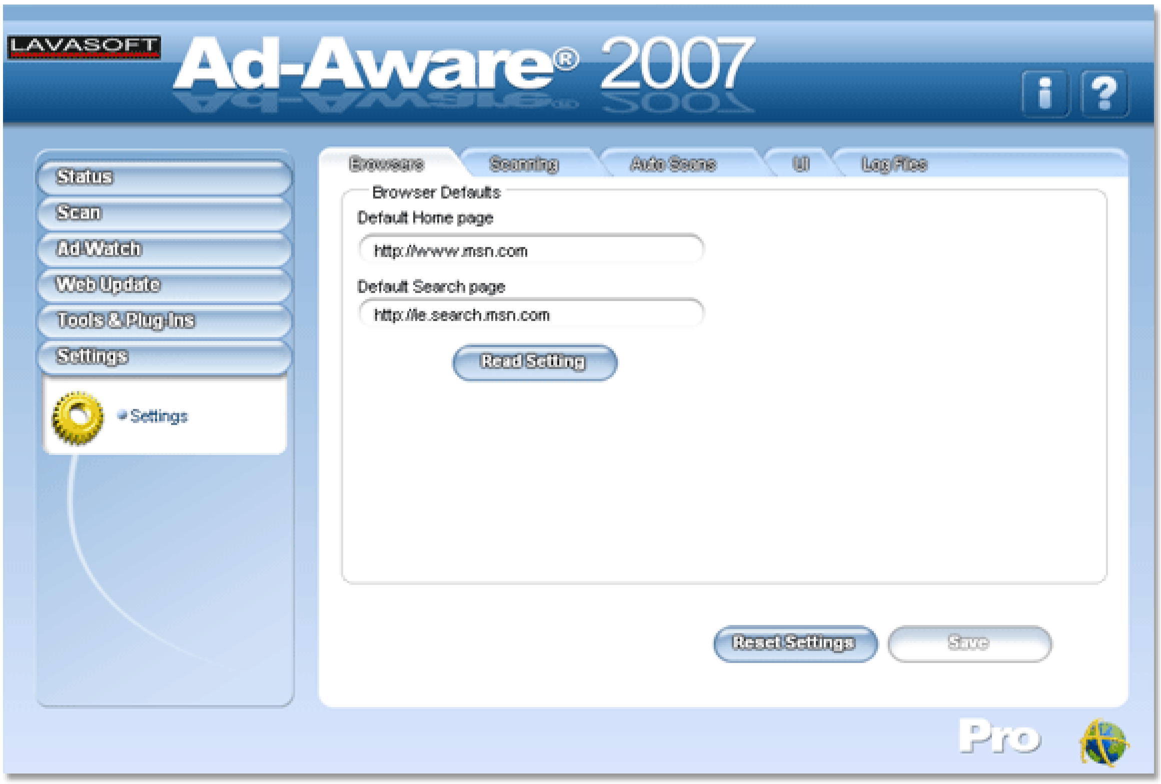
Click "Settings" in the main menu to open the Settings screen where you can customize Ad-Aware 2007 to fit your needs.

Use the tabs to navigate between different categories of settings.

Browsers

Browser Defaults

- Default home page: Ad-Aware 2007 uses the specified Internet Explorer home page when recovering from a browser hijack. When you click "Read Setting," your current Internet Explorer home page setting will be used.
- Default search page: Ad-Aware 2007 uses the specified Internet Explorer search page when recovering from a browser hijack. When you click "Read Setting," your current Internet Explorer search page will be used.



Browser Defaults

Default Home page

http://www.msn.com

Default Search page

http://ie.search.msn.com

Scanning

Processes Detected During Scan

- Unload malicious processes & modules: This allows Ad-Aware 2007 to close any currently running process or module that is recognized by the Detection Database. If this setting is disabled, the recognized process or module will continue to run during the remainder of the scan. Deactivation of this option does not imply that Ad-Aware 2007 will not be able to remove the executable if selected for removal by the user, just that removal will happen more efficiently if the process has already been stopped.
- Remove malicious LSPs: LSPs, or layered service providers, are often exploited by spyware and adware. If selected, Ad-Aware 2007 will remove LSPs in detection.

Scanning Options

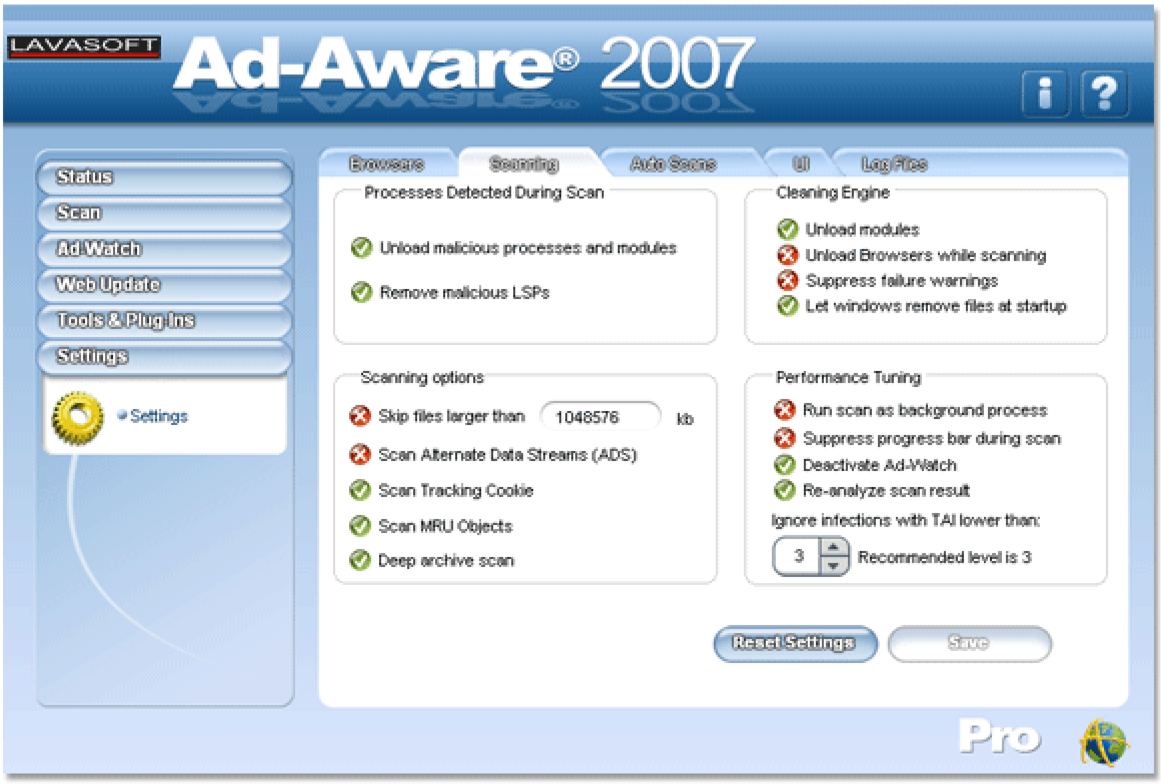
- Skip files larger than "X" kb: Ad-Aware 2007 will skip files that are larger than the specified value. This is most useful for those with large (clean) files such as music or digital imaging files. This will decrease scanning time.
- Scan Alternate Data Streams (ADS): Ad-Aware 2007 will scan files and investigate ADS streams for malicious objects.
- Scan tracking cookies: Ad-Aware 2007 will scan for tracking cookies in Internet Explorer, Mozilla Firefox, and Opera.
- Scan MRU objects: Ad-Aware 2007 will scan MRU (Most Recently Used) objects.
- Deep archive scan: Ad-Aware 2007 will thoroughly scan archives to ensure authenticity.

Cleaning Engine

- Unload modules: Ad-Aware 2007 will unload running process modules that have matches in the Detection Database.
- Unload browsers while scanning: Any browsers that are open will be closed before a scan is performed.
- Suppress failure warnings: Messages with certain objects that cannot be removed will be suppressed.
- Let Windows remove files at start-up: If it is necessary to restart your computer to remove a file, Ad-Aware 2007 will request that the files be removed during the next system restart. Ad-Aware 2007 will instruct Windows to remove these files at start-up.

Performance Tuning

- Run scan as a background process: Forces Ad-Aware 2007 to run in the background with a lower priority level. This allows other running programs to obtain more processor time.
- Suppress progress bar during scan: When a scan is performed, Ad-Aware 2007 will not show the progress bar on the "Performing Scan" screen.
- Deactivate Ad-Watch: Ad-Watch will be deactivated when Ad-Aware 2007 scans your system.
- Re-analyze scan result: After a scan is completed, Ad-Aware 2007 will re-analyze the findings before presenting them.
- Ignore infections with TAI lower than "X": Items that receive a TAI (Threat Analysis Index) level less than 3 are considered to be low risk threats. You may choose to ignore low risk infections.



Processes Detected During Scan

✓ Unload malicious processes and modules

✓ Remove malicious LSPs

Cleaning Engine

✓ Unload modules
✗ Unload Browsers while scanning
✗ Suppress failure warnings
✓ Let windows remove files at startup

Scanning options

✗ Skip files larger than 1048576 kb
✗ Scan Alternate Data Streams (ADS)
✓ Scan Tracking Cookie
✓ Scan MRU Objects
✓ Deep archive scan

Performance Tuning

✗ Run scan as background process
✗ Suppress progress bar during scan
✓ Deactivate Ad-Watch
✓ Re-analyze scan result

Ignore infections with TAI lower than:

3 Recommended level is 3

Auto Scans

System

- Automatically remove infection with TAI higher than "X": Allows you to automatically remove infections above a specified TAI rating in a start-up scan.
- Close Ad-Aware 2007 after start-up scan: Once the scan is complete and any detected objects have been handled, Ad-Aware 2007 will automatically shut down.
- Update Definitions File before scanning: Automatically checks for updates to the Detection Database before scanning. If an updated file is available, it is automatically downloaded to your computer

Start-Up Scan

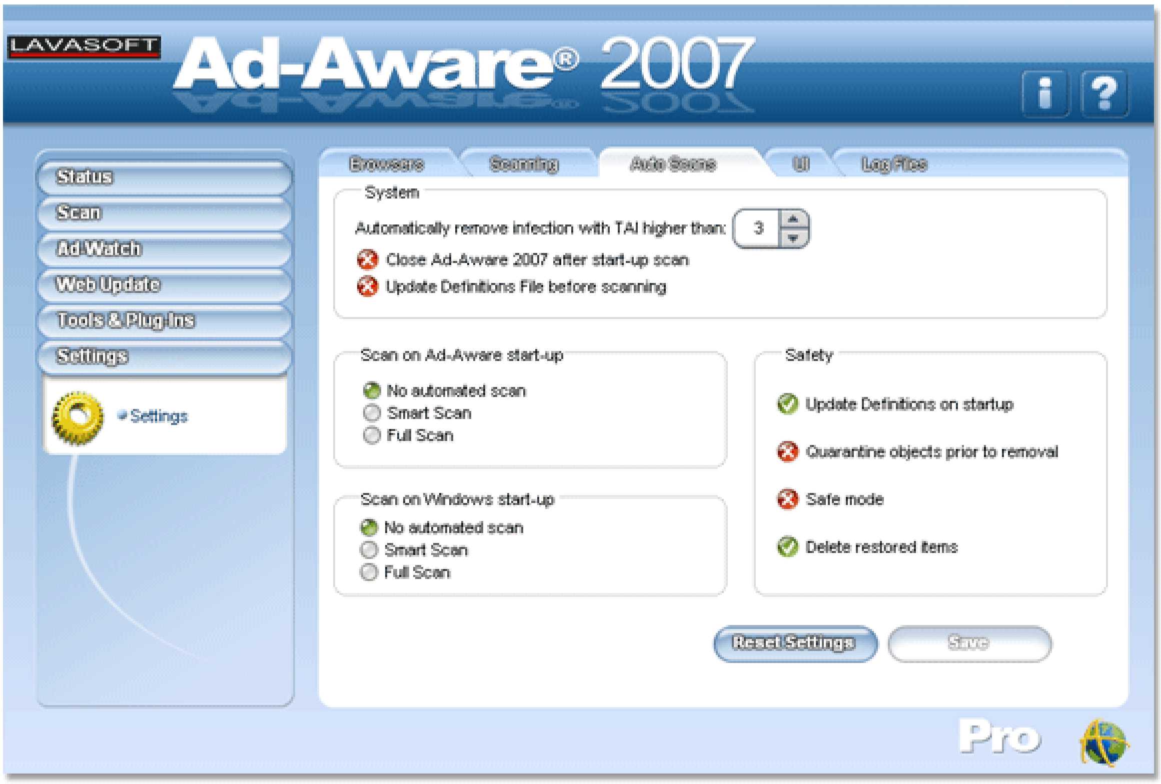
- No automated scan: No automated scanning will be performed when you start Ad-Aware 2007. This is independent from command line parameters.
- Smart Scan: A Smart Scan will be performed when you start Ad-Aware 2007.
- Full Scan: A Full Scan will be performed when you start Ad-Aware 2007.

Windows Start-Up Scan

- No automated scan: No automated scanning will be performed at Windows start-up. This is independent from command line parameters.
- Smart Scan: A Smart Scan will be performed at Windows start-up.
- Full Scan: A Full Scan will be performed at Windows start-up.

Safety

- Update Definitions on start-up: When you start Ad-Aware 2007, the program will check for Definitions File updates.
- Quarantine objects prior to removal: Quarantines objects that have been marked for automatic clean.
- Safe mode: A dialog box requesting confirmation will be displayed when altering (removing, quarantining, etc.) objects.
- Delete restored items: After the objects in Quarantine are restored, the quarantine file is deleted. If disabled, the quarantine file will remain on the system even after restoring its contents.



System

Automatically remove infection with TAI higher than: 3

☒ Close Ad-Aware 2007 after start-up scan

☒ Update Definitions File before scanning

Scan on Ad-Aware start-up

● No automated scan

○ Smart Scan

○ Full Scan

Scan on Windows start-up

● No automated scan

○ Smart Scan

○ Full Scan

Safety

✓ Update Definitions on startup

☒ Quarantine objects prior to removal

☒ Safe mode

✓ Delete restored items

User Interface

Miscellaneous

- Integrate into Windows Explorer: This setting allows you to use the right-click menu to scan a file or folder with Ad-Aware 2007.
- Dump exceptions to disk: If an exception occurs that cannot be handled, Ad-Aware 2007 will append to (or create) a special log file for later trouble-shooting and/or product support.
- Write protect system files: Ad-Aware 2007 will write-protect certain system files after repairing them, such as the Hosts File.
- Use grid lines in results list: Display grid lines in the scan result lists.
- Use Tool tips: Display tool tips for the Ad-Aware 2007 user interface.

Sound

- Play a sound if scan locates an infection: Check the box to have Ad-Aware 2007 play a sound at the end of a scan if any critical objects are detected. You can choose a wave-file to be played when content is detected. Any file with a .wav extension can be used.

Menu Animation

- No animation: The Ad-Aware 2007 main menu will have no animation when selecting headings.
- Slow animation: The Ad-Aware 2007 main menu will be set to slow animation when selecting headings.
- Normal animation: The Ad-Aware 2007 main menu will be set to normal animation when selecting headings.

Skin

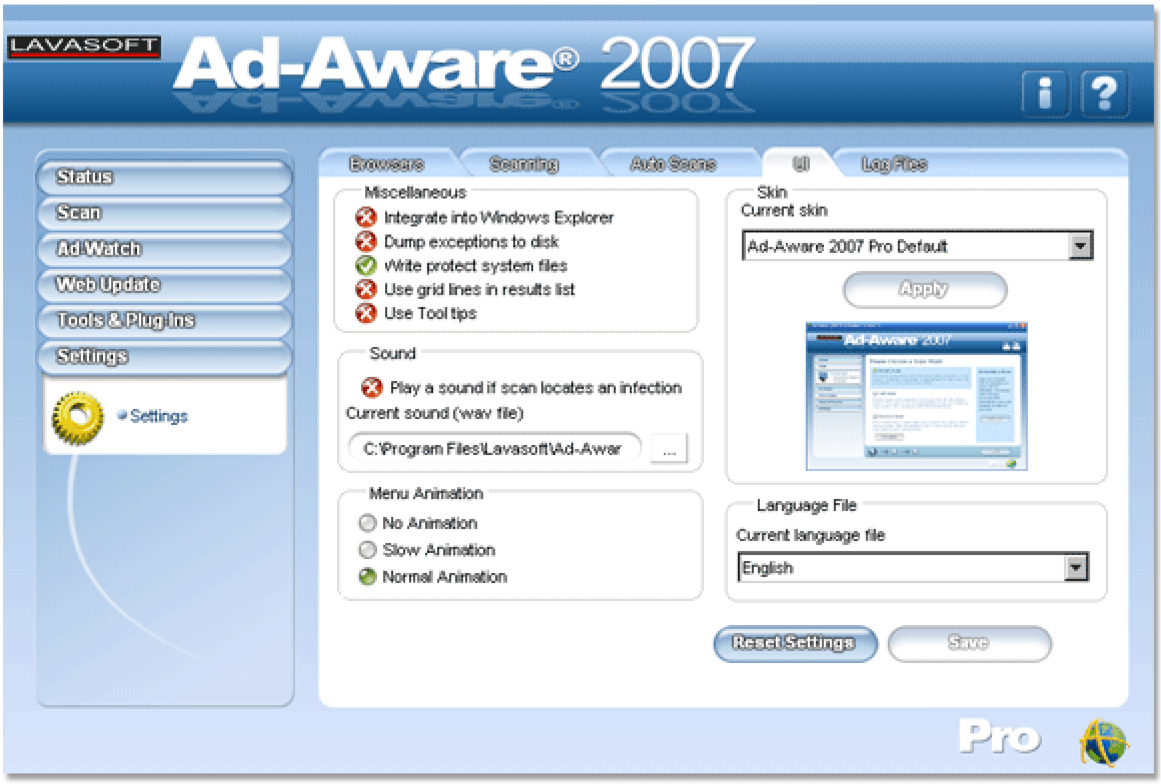
You can change the look of the program by changing skins. Skins are free of charge and can be downloaded from Lavasoft's website. (Ad-Aware SE skins are not compatible with Ad-Aware 2007). To download skins for Ad-Aware 2007, check for skins on the Lavasoft website, and follow the installation instructions.

When you restart Ad-Aware 2007, under "Current skin" in the Settings menu, you will be able to select the skin that you would like to use from the drop-down menu. Click "Apply" to apply the skin you selected.

Language File

You can change the interface of the program to the language of your choice by installing the Language Pack for Ad-Aware 2007 when it becomes available. The Language Pack is free of charge and can be downloaded from Lavasoft's website. When it becomes available, in order to download the Language Pack for Ad-Aware 2007, go to the Language Pack page on the Lavasoft website, and follow the installation instructions.

When you restart Ad-Aware 2007, under "Current language file" in the Settings menu, you will be able to select the language of your choice from the drop-down menu. Click "Save" to save your settings.



Miscellaneous

☒ Integrate into Windows Explorer

☒ Dump exceptions to disk

☑ Write protect system files

☒ Use grid lines in results list

☒ Use Tool tips

Sound

☒ Play a sound if scan locates an infection

Current sound (wav file)

C:\Program Files\Lavasoft\Ad-Awar ...

Menu Animation

○ No Animation

○ Slow Animation

● Normal Animation

Skin

Current skin

Ad-Aware 2007 Pro Default

Language File

Current language file

English

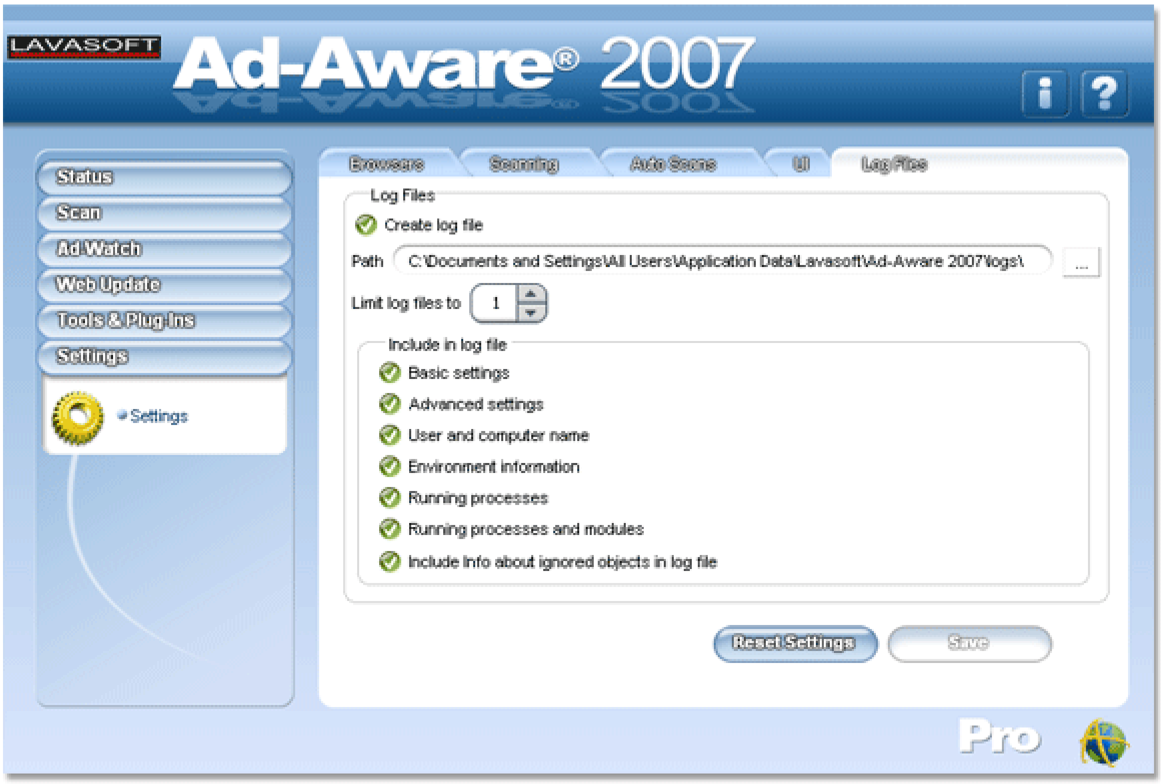
Log Files

Log Files

- Create log file: Check the box to have Ad-Aware 2007 create log files from your scans. Use the browse feature to locate the folder you wish to store the log files in. Click on the folder and navigate to your chosen location.
- Limit log files to "X": Allows you to set a limit to the amount of log files created. This may be useful so that log files do not take up added hard drive space. The default setting limits your log files to one.

Include in Log file

- Basic settings: Includes basic settings information in the log file.
- Advanced settings: Includes detailed settings information in the log file.
- User and computer name: Includes the computer's name and the user name currently logged on in the log file.
- Environment information: Includes system related as well as Ad-Aware 2007 specific environment information in the log file.
- Running processes: Includes a list of all running processes in the log file.
- Running processes and modules: Includes a list of all running processes and their associated modules in the log file.
- Include info about ignored objects in log file: Includes information about detected objects that you have added to the Ignore List in the log file.



Log Files

✓ Create log file

Path C:\Documents and Settings\All Users\Application Data\Lavasoft\Ad-Aware 2007\logs\

Limit log files to 1

Include in log file

✓ Basic settings
✓ Advanced settings
✓ User and computer name
✓ Environment information
✓ Running processes
✓ Running processes and modules
✓ Include Info about ignored objects in log file

Using Command Line Parameters

Ad-Aware 2007 can be operated without using the graphical user interface (GUI). It can be controlled by using command line parameters. UNC paths are supported.

Example:

```
>Ad-Aware2007.exe /Smart /Silent /Cookies
```

Ad-Aware will run in the background (without the GUI) and perform a Smart Scan with cookie scan turned on.

Scanning Parameters

`/Full`

Performs a Full Scan. If set, this parameter will override all other scanning parameters, except the optional Full Scan settings: /Cookie /ADS and /MRU.

`/Smart`

Performs a Smart Scan. If set, this parameter will override all other scan parameters except the optional Smart Scan settings: /Cookie /ADS and /MRU, and /Full, which takes precedence over /Smart.

`/Processes`

Scans all active processes.

`/Reg`

Scans the registry.

`/RegPE`

Scans registry executables.

`/Hosts`

Scans the Hosts file.

`/exe`

Scans only executable files.

`/zip`

Scans archives

`/deepzip`

Deep-scans archives.

`/Spanned`

Scans spanned files.

`/ukpds`

Unloads all malicious programs. The /process option has to be set for this option to have effect.

`/PBH`

Scans for possible browser hijacks.

`/LSP`

Scans Layered Service Providers.

`/Path [filepath]`

Sets a folder to be scanned. If you want to scan more than one folder, you will have to use this parameter for each folder. Usage: `/Path C:\Windows\ /Path C:\Program Files\`

`/Cookies`

Scans Tracking Cookies.

`/ADS`

Scans Alternate Data Streams.

`/MRU`

Scans Most Recently Used (MRU) lists.

Other Scanning Options

`/FileSize [0]`

Sets the maximum size of the files to be scanned in kilobytes. If it is not set, it will default to 0 (i.e. all files will be scanned). Usage: `/FileSize 4000`

`/ScanTAI [1-10]`

Sets the lowest TAI to scan for. If not set, TAI 3 will be used. Usage: `/ScanTAI 5`

Cleaning

`/Clean`

Detected malware will be cleaned.

`/CleanTAI [1-10]`

Set the lowest TAI to clean.Usage: `/CleanTAI 4`

`/NoQuarantine`

Infections will not be quarantined before removal. If this option is not set, all infections will be quarantined.

Updates

`/Update`

Performs a Web Update to look for a new Definitions File. If there is a newer version it will be downloaded and installed.

`/Backup [filename]`

Creates a backup of the current Definitions File before updating. Usage: `/Backup defs.bak`

Miscellaneous

`/Silent`

Runs Ad-Aware 2007 without showing the graphical user interface and performs a scan that automatically quarantines any detected objects.

`/Stat [filename]`

Creates a file containing statistics, version numbers and settings for the scan.
Usage: `/Stat scanstats.txt`

Uninstall Ad-Aware 2007

You can use one of the methods below to uninstall Ad-Aware 2007.

Uninstaller

- Go to the "Lavasoft Ad-Aware 2007" folder in your Start menu.
- Run "Uninstall Ad-Aware 2007".
- Verify uninstalling by selecting "Yes."
- When the program exits, Ad-Aware 2007 has been uninstalled.

Control Panel

- Go to the Control Panel.
- Run "Add or Remove Programs".
- Select Ad-Aware 2007 in the list and click the "Change/Remove" button
- Verify uninstalling by selecting "Yes."
- When the program exits, Ad-Aware 2007 has been uninstalled.

Lavasoft Support Center

Under the Support menu tab at www.lavasoft.com, you can access the FAQs, the Support Forums, and the Support Center. Access to the Support Center is only available to customers who have purchased Ad-Aware 2007 Plus, Ad-Aware 2007 Pro and Ad-Aware SE Enterprise.

FAQs

The FAQs provide you with answers to some of the most frequently asked questions about Lavasoft products. For your convenience, we have sorted the Frequently Asked Questions (FAQs) by topic to include technical, sales, and reseller sections.

Support Forums

In the Lavasoft Support Forums, at www.lavasoftsupport.com, you will find useful information about our products, browse solutions to problems, and post questions to be answered by Lavasoft staff, experienced professionals and knowledgeable Ad-Aware users.

Support Center

Your purchase of Ad-Aware 2007 provides you with unlimited access to Lavasoft's Support Center. By logging into the Support Center, you have easy access to your user information (your license and personal information), the Customer E-Store (ordering instructions, version update information, etc.) product resources (product downloads and manuals) and support (technical and sales support).

Through the Support Center, you can contact the Lavasoft Support Center staff by e-mail. After logging in to the Support Center, send in a Technical Support or Sales Support inquiry.

We provide large corporations and Enterprise customers with Point of Contact (POC) support. Service Level Agreements (SLA's) are also available upon request.

Lavasoft Security Center

Using Lavasoft's Security Center, available from our website, you are able to submit new suspicious files for review, access resources for beta testers and for vendors, get a deeper understanding of the Threat Analysis Index, visit the Spyware Education Center, and download Definitions File updates from the Detection Database.

Threat Analysis Index

Information about the items detected by Ad-Aware 2007 can be found in Lavasoft's Security Center, in the Threat Analysis Index pages.

When you scan your computer using Ad-Aware 2007, potential threats are analyzed using specific criteria. The weights of the criteria are tallied, to give the threat a specific Threat Analysis Index (TAI) level. This determines if the threat should be added to our Detection Database, and gives you the power to make quick decisions about what to do with the detected spyware and malware.

The TAI point system is based on a 10-point scale, with 1 representing the lowest threat and 10 representing the highest. A minimum TAI value of 3 is required before the malware is put into detection at the Lavasoft Security Center.

When creating the TAI level, the behavior of the threat carries a stronger weight than its technical aspects; if the malware secretly attaches without your full understanding and approval, then the threat is automatically given higher TA points. Applications that are difficult to remove and cause system instability due to poor coding but do not contain any further violations are not considered for inclusion in the Detection Database.

Information on TAI categories and TAI analysis criteria can be found on the Lavasoft website. See more information on the Threat Analysis Index.

Spyware Education Center

The Spyware Education Center is a resource for everyone- from computer novices to spyware experts- to find out more about one of the most menacing technological applications of the cyber era. Visit the Spyware Education Center to read about the history of spyware, ways to protect yourself, a glossary of key terms, and spyware statistics.

Purchasing Additional Lavasoft Products

Please use the following links to our website for more information on Lavasoft products.

Home Users

Please visit our Select Your Product page. You can also browse the Product Comparison Chart to find the Lavasoft product that is right for you.

For sales questions, please contact our Worldwide Sales Department. (This address is for sales questions only; technical support questions will not be answered.)

Business Users

Please visit our Select Your Product page where you can browse products in the Small Business or Enterprise category. You can also use the Product Comparison Chart to find the Lavasoft product that is right for you.

If you have joined our global network of Lavasoft partners or if you are a registered reseller, you may use the resources available by logging in to the Partner Center or Reseller Center.

For sales questions, please contact our Worldwide Sales Department. (This address is for sales questions only; technical support questions will not be answered.)

Academic & Non-Profit

At Lavasoft, we realize that it is sometimes difficult for students and non-profit organizations to commit money towards technology upgrades. Because we strongly believe that everyone has the right to privacy and security of their personal information, we offer a 50 percent discount off our products for students and non-profit organizations. For more information, please visit the Academic/Non-Profit page.

Support Center

Visit the Lavasoft Support Center for a convenient way to upgrade your software, communicate with Support Center staff through e-mail, and have access to important product resources.

Glossary

To view a glossary of key terms frequently associated with spyware and adware, please visit Lavasoft's Spyware Education Center. Lavasoft is one of the founding members of the Anti-Spyware Coalition (ASC), which annually publishes security industry reports; Lavasoft's glossary is a condensed version of the ASC's terms and definitions.