Ad-Aware®

Anniversary Edition

User Manual

Table of Contents

What Is Ad-Aware Anniversary Edition?

Ad-Aware is Lavasoft's industry leading anti-malware solution that allows you to combat stealthy online threats and the latest advancements by cyber criminals. Ad-Aware protects you from spyware and malware that secretly takes control of your computer, resulting in aggressive advertising pop-ups, sluggish computer activity and even identity theft through stolen private information. Ad-Aware allows you to root out hazardous content on your system, clearly identify the threat level, and gives you the ability to remove or block harmful applications and processes, so that your private information remains right where it should - under your control.

2009 marks Lavasoft's 10 year anniversary of providing computer users with the power to protect their privacy. Building on 10 years of advanced malware detection, the latest version of Ad-Aware, Ad-Aware Anniversary Edition, provides powerful malware detection, removal and clean-up without loading down your system's resources.

Ad-Aware Anniversary Edition is available in Free, Plus, and Pro versions. Ad-Aware Free features anti-spyware protection and now includes integrated Ad-Watch Live! Basic real-time protection. The Plus and Pro versions boost security with comprehensive malware protection – anti-spyware AND anti-virus protection means you are protected from over 2 million threats, with advanced real-time protection and behavior-based heuristical detection to find and block unknown and emerging threats.

Ad-Aware Anniversary Edition Features

- **Ad-Watch Live!** – Integrated Ad-Watch Live! real-time protection detects deceptive malware applications before they integrate into your PC and attack your personal information. (**Free**, **Plus**, **Pro**).

- Ad-Watch includes:
  - **Ad-Watch Real-time Process Protection:** Ad-Watch suspends suspicious files and blocks malicious processes that try to start or run on your system - to prevent them from further integration in your system - giving you the power to allow or block the process.
  - **Ad-Watch Real-time Registry:** Advanced detection of attempted registry changes, a favorite target for many malware distributors. Ad-Watch alerts you when a program tries to make changes to your registry, giving you the power to block or allow access to that program.
  - **Ad-Watch Real-time Network:** Ad-Watch monitors outgoing network traffic and blocks connections to blacklisted IP addresses and known malicious websites to identify and stop active threats.

- **Ad-Watch Live! Basic** – Real-time process protection blocks malicious processes and infected files that try to start or run on your system. (**Free**)

- **Ad-Watch Live! Advanced** – Real-time registry protection and process protection including behavior-based heuristics scanning. (**Plus**)

- **Ad-Watch Live! Expert** – Includes an additional layer of security by blocking connections to blacklisted IP addresses. It also adds process protection including behavior-based heuristics scanning, registry protection, and real-time network protection. (**Pro**)

- **Comprehensive Malware Protection** – Protection against spyware, Trojans, rootkits, hijackers, keyloggers, and more. (Free) Advanced, multi-layered malware protection with anti-spyware and anti-virus. (**Plus**, **Pro**)

- **Rootkit Removal System** – Advanced anti-rootkit technology protects you from hidden threats and stealth attacks that are designed to gain access to your system by avoiding detection. (**Free**, **Plus**, **Pro**)

- **Detect, Remove AND Clean** – A step beyond simply detecting and removing malware, Ad-Aware intelligently cleans your system by removing all traces of the infection. (**Free**, **Plus**, **Pro**)

- **Automatic Updates** – Protect against the latest forms of malware with free software feature updates and definitions file (threat) updates throughout the license duration. (**Free**, **Plus**, **Pro**)

- **Lavasoft SmartSet** – Get started quickly and easily by using Lavasoft SmartSet. Based on expert recommended settings, we have configured Ad-Aware to make scanning and cleaning your computer as easy as possible. No need to stress – your Ad-Aware is good to go. (**Free**, **Plus**, **Pro**)

- **External Drive Scanning** – Scan your external storage device, iPod, DVD's, USB's, or any other drives that you connect to your PC for an additional layer of security. (**Free**, **Plus**, **Pro**)

- **Customizable Profile Scans** – Easily create personalized scan profiles so that Ad-Aware only scans areas that you select. Save time by scanning areas where known malicious programs are located, or choose from 13 different sections to scan, including critical sections, folder selection, only executables, compressed files, and the Windows registry. (**Free**, **Plus**, **Pro**)

- **ThreatWork** – Submit suspicious files to Lavasoft researchers for analysis in just one easy click. ThreatWork is an alliance of global anti-malware security volunteers actively fighting online threats. (**Free**, **Plus**, **Pro**)

- **TrackSweep** – Control your privacy by erasing tracks left behind while surfing the web on multiple browsers, including Internet Explorer, Firefox, and Opera, with one easy click. (**Free**, **Plus**, **Pro**)

- **System Restore Point** – Set a system restore point so you can clean your PC without fear of obstructing your operating system – revert to a previous state in the event of a problem. (**Free**, **Plus**, **Pro**)

- **Substantially Reduced Use of Computer Resources** – Tread lightly on your system's resources with dramatic improvements to the memory usage. (**Free**, **Plus**, **Pro**)

- **Easy to Download, Install and Use** – Effortlessly maneuver the complexities of malware detection and removal with our new, polished, user-friendly interface. (**Free**, **Plus**, **Pro**)

- **Pin-Point Scanning** – Easily identify whether suspicious files are safe or malicious - right-click any file or folder to perform an immediate Ad-Aware scan. (**Free**, **Plus**, **Pro**)

- **Background Scanning** – Save resources by closing Ad-Aware while scanning your computer – keep working while a scan is performed. (**Free**, **Plus**, **Pro**)

- **Tray Application** – Conveniently receive notifications and alerts and easily control Ad-Aware without running the full user interface. (**Free**, **Plus**, **Pro**)

- **Detailed Scan Logs** – Conveniently export scan reports as text files. (**Free**, **Plus**, **Pro**)

- Full Integration with Windows Security Center - Get Ad-Aware protection and status notifications through the Windows Security Center. (**Free**, **Plus**, **Pro**)

- **Free Technical Support** – Get immediate answers to your questions by easy, in-product access to the Lavasoft Support Center. Get support from an extensive international network of Lavasoft security analysts and volunteers at the Lavasoft Support Forums. (**Free**). Get unlimited support from our technical and customer support experts at the Lavasoft Support Center. (**Plus**, **Pro**)

- **Multi-language Support** – English, Dutch, Flemish, French, German, Italian, Portuguese, Spanish, Traditional Chinese, Simplified Chinese, and Japanese. (**Free**, **Plus**, **Pro**)

- **Behavior-based Heuristical Detection** – Extra Sensory Protection allows you to go a step beyond detecting known threats – the heuristical detection finds and blocks unknown and emerging threats by analyzing the process and assessing its behavior. (**Plus**, **Pro**)

- **Extensive Detection Database** – Ad-Aware now detects over 2 million known threats, with continuous pulse updates to guard your privacy against cyber attacks. (**Plus**, **Pro**)

- **The Scheduler** – Automatic scans set to your personalized schedule to optimize time and resources. (**Plus**, **Pro**)

- **Hosts File Editor** – An expert tool within Ad-Aware that allows you to take control of your web navigation by adding, deleting or making changes to the Hosts File to create Web navigational shortcuts and to block unsecure and harmful websites. (**Plus**, **Pro**)

- **AutoStart Manager** – Keep your computer running quickly with easy control over what programs start when your computer does - reducing the toll on your system that occurs when unnecessary programs are running. (**Pro**)

- **Network Drive Scanning** – Scan network drives so you can detect malware on any shared disks on your network, not just on your hard disk. (**Pro**)

- **Process Watch** – View an in-depth snapshot of all running processes and quickly stop known offenders. (**Pro**)

- **Command Line Support** – Manage Ad-Aware without launching the interface window. (**Pro**)

System Requirements

When installing Ad-Aware on Windows 2000, XP and Vista operating systems, please make sure you have administrative rights. 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.

Processor: Intel Pentium 600 MHz or better

RAM: Operating system + 100 MB

Hard Disk: 100 MB free space recommended

Operating Systems: Windows Vista (32- and 64-bit), Windows XP (32-bit), Windows 2000 Pro.

Install Ad-Aware

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

- Language Selection Window
  Choose your preferred language and click "Ok."

Welcome Screen
 Please read the welcome screen and review the Lavasoft Privacy Policy. Click "Next" to continue.

- Installation
   Please read the End User License Agreement before you proceed. When you have completed reviewing the agreement and if you agree to the terms, check the box next to "I accept the terms of license agreement." Press "Install" to continue with the standard installation of the software. To customize the installation, click "Customize Installation," choose the destination folder and select whether to add the Ad-Aware shortcuts or not. Click "Next" and select whether to install Ad-Watch Live! or not. Click "Next" and press "Install" to continue with the Custom installation. After the files finish copying, you will receive a confirmation message that the installation was successful.

- Installation Complete
  Your computer must be restarted to complete the installation. Click the option to "Restart now." At this point, you also have the option to enter your e-mail address to receive Lavasoft News and special offers. Click "Finish" to complete the installation process. Your computer will restart and Ad-Aware will be completely installed.

Registering Your Product

If you have bought Ad-Aware 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.

If you are using the Ad-Aware Free version, on the "Main Status" screen, click the "Register" button to access the activation window. If the program is already activated and you want to upgrade or extend your license, on the "Main Status" screen, click the "Manage License" button to access the activation screen.

Manage License

Enter your serial number in the "Serial number" field and press the "Register" button. The program will then activate your license and the "Registration Successful" window will open. Click "OK" to continue.

The "Current License" window displays the information about your license. Your license type (Ad-Aware Free, Plus or Pro) and license expiry date are shown.

The hardware fingerprint is a signature of your PC system. At activation, your serial key is associated with this hardware fingerprint. If you need to transfer your license to a new PC, please contact our support department with this hardware fingerprint and your license information.

If you do not have a serial key and want to buy a license, simply click "Buy License" to open the Lavasoft Store where you will find a full description of the extended functionality of the Plus and Pro versions.

No serial number is required to activate Ad-Aware Free. Click "Close" to continue using Ad-Aware Free.

Main

Click the "Main" menu icon to view the main status window.

Main Status

The Main Status screen displays a snapshot of the latest status of Ad-Aware's main features.

At a glance, you can see if the software is up to date, the latest scan status, Ad-Watch Live! events, access the configuration settings, schedule a scan, view the latest industry news, manage your license and contact our support team with technical inquiries.

When you click "Web Update", the Update Manager will open, then download and install any available updates. Before you scan your computer, you should always be sure to have the latest updates by performing a Web Update. You can configure the software to automatically download and install available updates in the update settings.

Click the "Scan System" icon to open the Scan Mode screen.

Click the "Ad-Watch Live!" icon to open the Ad-Watch Live! real-time protection screen.

Click the "Schedule a Scan" icon to configure a scheduled scan.

Click the "Manage License" button to access the activation screen.

Click "Settings" to open the Settings screen where you can customize Ad-Aware to fit your needs. The settings are context sensitive, meaning that when you click on settings for a particular feature, the settings for that feature open. Use the tabs in the sub-menu to navigate between different categories of settings.

Main Menu Buttons

Only the menu icon for the screen being displayed will be colored, the other menu icons will be grayed out.

Click "Settings" to open the Settings screen where you can customize Ad-Aware to fit your needs. The settings are context sensitive, meaning that when you click on settings for a particular feature, the settings for that feature open. Use the tabs in the sub-menu to navigate between different categories of settings.

Click the ''Main'' menu icon to view the main status screen.

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 a Profile Scan. We recommend updating Ad-Aware before scanning in order to have the latest Definitions File before you scan.


Click the "Ad-Watch" menu button to open the "Ad-Watch Live" screen. Ad-Watch Live! is the real-time monitor featured in Ad-Aware. The scanner in Ad-Aware detects and cleans malware and viruses from your system, but Ad-Watch goes a step further. From the moment your machine is turned on, Ad-Watch Live! is watching, actually catching these programs before they integrate and install on your PC. Ad-Watch Live! has three separate modules of protection: Processes, Registry and Network. Malicious processes and blacklisted IP addresses are automatically blocked. When a suspicious process or registry change is detected an Ad-Watch Live! 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.

Click the "Extras" menu button to open the extra toolbox screen.

Opens the Ad-Aware Anniversary Edition product manual.
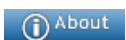
Opens copyright and contributor information about Ad-Aware Anniversary Edition.

Statistics

Shows statistics about the objects detected in previous scans.

Choose "Statistics" from the "Display" drop-down menu.

You can choose to display the total or specific time statistics.

Once selected, the "Scan Statistics" table will refresh.

The Scan log file is a detailed information log about the scan. It contains valuable information when troubleshooting errors.

Click "Export Scan Report" to open the scan log file as a text file, which you can save to your system.

Note: The Scan log file will open for the specific screen selected in the drop-down menu.

To reset statistics click the "Reset Statistics" button. This will clear the statistics starting from the moment you click this button.

Scan

Choose A Scan Mode

Smart Scan

The "Smart Scan" is a comprehensive, fast system check that scans the most critical sections of your system. The Smart Scan will scan your running programs and application starting points (applications that are configured to start automatically).This scan mode should be used for daily system maintenance.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, 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 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.

Profile Scan

The "Profile Scan" allows you to easily create personalized scan profiles so that Ad-Aware only scans areas that you select. Save time by scanning areas where known malicious programs are located, or choose from 13 different sections to scan, including critical sections, folder selection, only executables, compressed files, and the Windows registry. Free users can fully customize one default profile (including file selection, excluding anti-virus). Plus and Pro users have no limit to the number of new profiles they can customize.

Once you have selected a scan mode click "Scan Now." Ad-Aware will begin to scan your system, and the "Scanning System" screen will appear.

Scanning System

While Ad-Aware scans the system, the "Scanning System" menu displays the following:

Scan Mode: Type of scan.

Scan Time: Duration of scan.

Current Section: Section currently being scanned.

Objects Scanned: Amount of objects being scanned.

Objects Detected: Amount of detected objects.

Current Object: Current object being scanned.

Scan Results

The "Scan Results" screen shows information about the scan that you performed and information about the objects that were detected.

Ad-Aware 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. The detected objects are listed by family and are given a pre-selected Lavasoft "SmartSet" recommendation defined by Lavasoft experts. Lavasoft SmartSet makes scanning and cleaning as easy as possible by providing automatically configured settings for scans, and by providing recommended actions for found objects. Please review each detected item in the scan results screen before clicking "Perform Actions Now" as you have the final say in what to delete from your system.

In the "Scan Results" screen, detected objects are grouped by which family they belong to. The infection type, total number of objects, their TAI rating and the action to perform are also shown.

Family
A group of malicious programs that share similar code and behavior.

Infection Type
Provides more information about the behavior of the detected object.

Objects
The total number of detected objects for each family are listed.

TAI: Threat Analysis Index
Information about the items detected by Ad-Aware can be found in Lavasoft's Security Center, in the Threat Analysis Index pages. When you scan your computer using Ad-Aware, 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 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 TAI 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.

Action
To change an Action click on the drop-down menu under the Action heading.

The following actions are available.

Recommend: A pre-selected Lavasoft "SmartSet" recommendation defined by Lavasoft experts.

Custom: You can change the Action by clicking on "Custom Action" or by clicking on the description menu at the end of that particular Family.

The following Custom actions are available.

Remove: Delete the object from your system.

Repair: Ad-Aware will attempt to repair the infected file.

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.

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

Allow/Leave On System: Allow the object to stay on the system. During the next scan, the object will be detected again.

System Restore Point
Before performing actions on 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. Select "Set System Restore Point" to create a backup, or restore point, of vital system configurations and files. You should choose to create a system restore point prior to performing actions on objects that you are unsure of removing.

Select the required action for each object from the drop-down menu and then click "Perform Actions Now".

Ad-Aware will apply the required action for each detected object and present you with 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 scanned, removed, repaired, left on the system, added to the ignore list, and quarantined. The "Outcome of Cleaning" is also shown.

Outcome of Cleaning

Successful: The specified action applied to this object was successful.

Reboot Required: If it is necessary to restart your computer to remove a file, Ad-Aware will request that the files be removed during the next system restart. Ad-Aware will instruct Windows to remove these files at start-up.

Clean Failed: The cleaning action failed. If this occurs we recommend that you run a full system scan in Windows safe mode.

The scan log file is a detailed information log about the scan. It contains valuable information when troubleshooting errors.

Click on the "Export Scan Report" to open the scan log file as a text file, which you can save on your PC.

Scan Log File

Contents of Scan Log File:

Log File Date
Ad-Aware Version
Extended Engine Version

Definitions Database Information:
Information on the Latest Definition File
Lavasoft Definition File
Extended Engine Definition File

Scan Results:
Scan Profile Name
Objects Scanned
Objects Ignored
Objects Detected

Action Taken:
Lists the action taken for the detected objects

Scan and Cleaning Complete:
Success/Stopped/Failed

Settings:
List of Ad-Aware Scan Settings

System Information:
Lists the system information

Windows Startup Mode:
Start Up Items
Services
Running Processes

Scheduler

Click "Scheduler" in the sub-menu to open the Scheduler. The Scheduler allows you to set up automated scans of your computer at set times on specific dates.

Scheduling Scans

Choose which scheduled scan to use/edit from the list or click "+" to add a new scheduled scan.

Type in the name for the scheduled scan and click "Ok".

To delete a scheduled scan, click "x".

1. **What:** Select which scan mode to use: Smart, Full or Profile. If you select a Profile scan, choose the Profile scan name from the drop-down menu.

2. **When:** Select the frequency of the scan: once, daily, weekly, monthly or at Windows startup. Select the date and start time of the scan.

3. **How:** Select whether the cleaning method is manual or automatic. If set to manual, when the scan is completed the scan results screen will be displayed, allowing you to manually choose the required action for each detected object. If set to automatic, when the scan is completed, the selected action to use: "Use recommended action" or "Remove detected objects", is applied to the detected objects.

Click "Save" to save the new scheduled scan.

Quarantine

Click "Quarantine" in the sub-menu to open the Ad-Aware Quarantine List.

Quarantine is used to isolate and backup objects detected during an Ad-Aware 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 Quarantine list. Objects stored in Quarantine do not pose a threat to your computer.

Quarantine lists objects by family, infection type and TAI rating.

Restore Quarantined Objects

In the Quarantine list, select the quarantined object or objects you would like to restore by selecting "Restore" from the Action drop-down menu. When you click "Perform Actions Now," the object/objects will be restored to your system.

Remove Quarantined Objects

In the Quarantine list, select the quarantined object or objects you would like to remove by selecting "Remove" from the Action drop-down menu. When you click "Perform Actions Now," the object/objects will be removed from your system.

Do Nothing

No action is applied - leave objects in Quarantine.

Click "Perform Actions Now" to apply the specified actions to the Quarantined objects in the list.

Ignore List
Click "Ignore List" in the sub-menu to open the Ad-Aware 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 to delete it. When you add items to the Ignore List, Ad-Aware will not detect them when your system is scanned.

The Ignore List lists types of objects together by family, infection type and TAI rating.

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 selecting the "Remove" option in the Action drop-down menu. When you click "Process Infections," the object/objects will be removed from the Ignore List, and Ad-Aware will detect these items in the next scan.

Do Nothing
No action is applied - leave objects in the Ignore List.

Click "Perform Actions Now" to apply the specified actions to the infections in the list.

Ad-Watch

Ad-Watch Live

Ad-Watch Live! provides three levels of protection for your PC:

Processes: Real-time process protection blocks malicious processes and infected files that try to start or run on your system.

Registry: Ad-Watch alerts you when a program tries to make changes to your Registry, giving you the power to block or allow access to that program. (Plus, Pro)

Network: Ad-Watch monitors outgoing network traffic and blocks connections to blacklisted IP addresses and known malicious websites to identify and stop active threats. (Pro)

The Ad-Watch Live! real-time protection screen gives you a simple overview of the Ad-Watch Live! real-time monitor;

It shows if real-time protection is on or off, and allows you to turn each module on or off by simply clicking on the icon.

Note: If the icon is disabled, then the software has not being activated or the feature is not included in the version you have installed.

It also shows you the latest detected processes, accessed registry areas and blocked IP addresses.

Click "View Detailed Report" to open a text log file which includes the full list of blocked processes, registry areas or blocked IP addresses.

You can manage the rules for each module of Ad-Watch Live! by choosing the sub-menu or by clicking "Edit Rules."

Process Rules

For each detected malicious or suspicious process, you can change the "Action" from the drop-down menu.

Inform: The process is detected as malicious and you will be informed that is was blocked every time it attempts to run.

Block: The process is always blocked and no Ad-Watch notification will appear.

Allow: The process is always allowed to run and no Ad-Watch notification will appear. Warning! Only use this action if you are sure that the process is safe.

Click "Save" to apply changed actions to the processes in the list.

Registry Rules

Every application that tries to change a registry area will be shown in this list. Ad-Watch Live! Registry protection allows you to protect the following areas of your registry:

- **Startup Settings:** Applications that are configured to start automatically.
- **Windows File Associations:** Where Windows recognizes the file name extension and opens the file in the program that is associated with that file name extension. (For example: to associate ".psd" with Photoshop, or "html" with your browser of choice).
- **Browser Helper Objects:** A program or plug-in that loads each time the Microsoft Internet Explorer Web browser is launched.
- **Windows Security Restrictions and Policies:** Provides administrators with a way to identify and control the ability of particular software to run on a computer.
- **Internet Browser Settings:** Your Internet browser 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.
- **Interception of Internet Traffic:** This occurs when information sent from your PC is intercepted by someone other than the intended recipient.

For every application that is trying to change the registry area, there are three different 'Access Rights' actions. Use the drop-down menu to change the action.

Inform: The application is trying to change the registry area. An Ad-Watch notification will appear allowing you to allow or block this change.

Block: The application is always blocked from changing the registry area and no Ad-Watch notification will appear.

Allow: The application is always allowed to change the registry area and no Ad-Watch notification will appear. Warning! Only use this action if you are sure that the process is safe.

Click "Save" to apply changed actions to the processes in the list.

Network Rules

Real-time Network protection is designed to detect connections to blacklisted IP addresses. When any application connects to a blacklisted IP address that is detected as malicious, the Ad-Watch notification will inform you that it was blocked.

For every application that is connecting to a blacklisted IP there are two different 'Actions'. Use the drop-down menu to change the action.

Block: The connection to this blacklisted IP address is always blocked and no Ad-Watch notification will appear.

Allow: The connection to this blacklisted IP address is always allowed and no Ad-Watch notification will appear. Warning! Only use this action if you are sure that the connection to this IP address is safe.

Click "Save" to apply the specified actions in the list.

Extras

TrackSweep

Select "TrackSweep" from the sub-menu to access Ad-Aware's TrackSweep tool.

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

By checking the boxes next to the items of your choice and clicking "Sweep Now", the tracks left behind when you surf the Internet will be cleaned from Internet Explorer, Firefox, and Opera web browsers.

Note: Please close the browser in order for it to be cleaned.

Toolbox

Click "Toolbox" in the sub-menu to open Ad-Aware's extra "Tools". These tools are stand-alone applications that add extra functionality to Ad-Aware.

Click "Start" to start the extra application.

Process Watch

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.
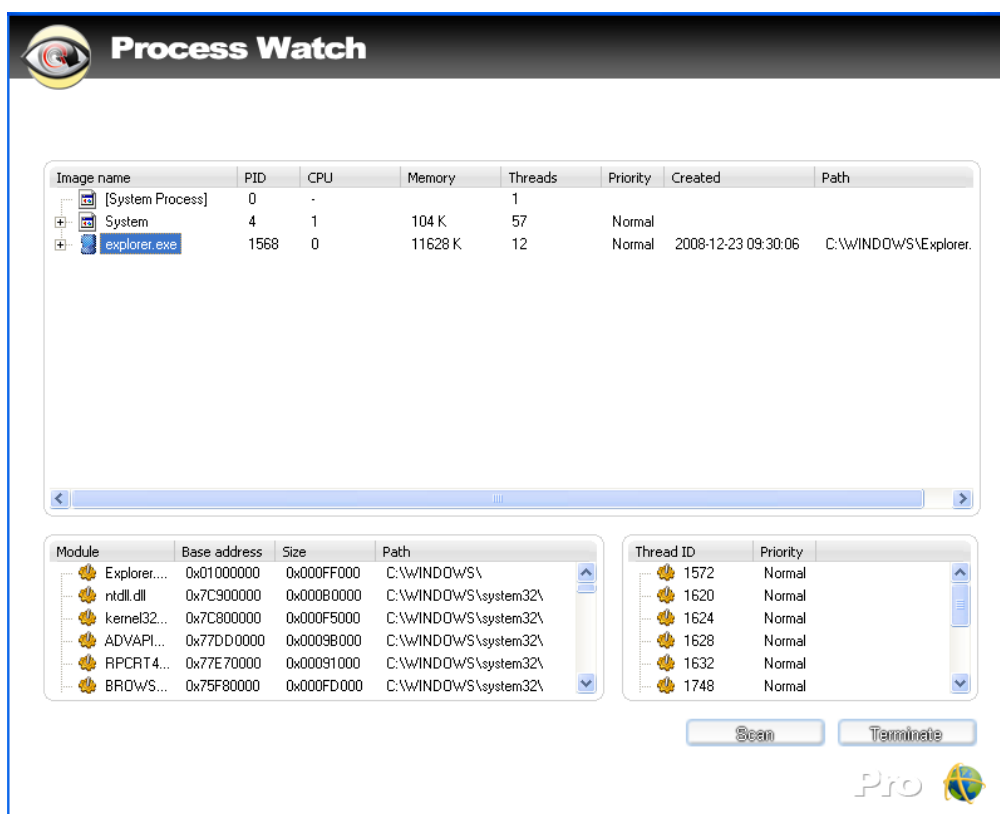
Using Process Watch

When the Process Watch tool 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.

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 from 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:** Priority level of time-critical tasks that must be executed immediately.
    - **Above Normal*:** Priority level above the normal level.
    - **Normal:** Priority 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.)

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.

Host File Editor

The Hosts File Editor allows you to block advertisement sites, reverse browser hijack entries, create navigation shortcuts, assist with parental controls and make other exceptions to regular 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.
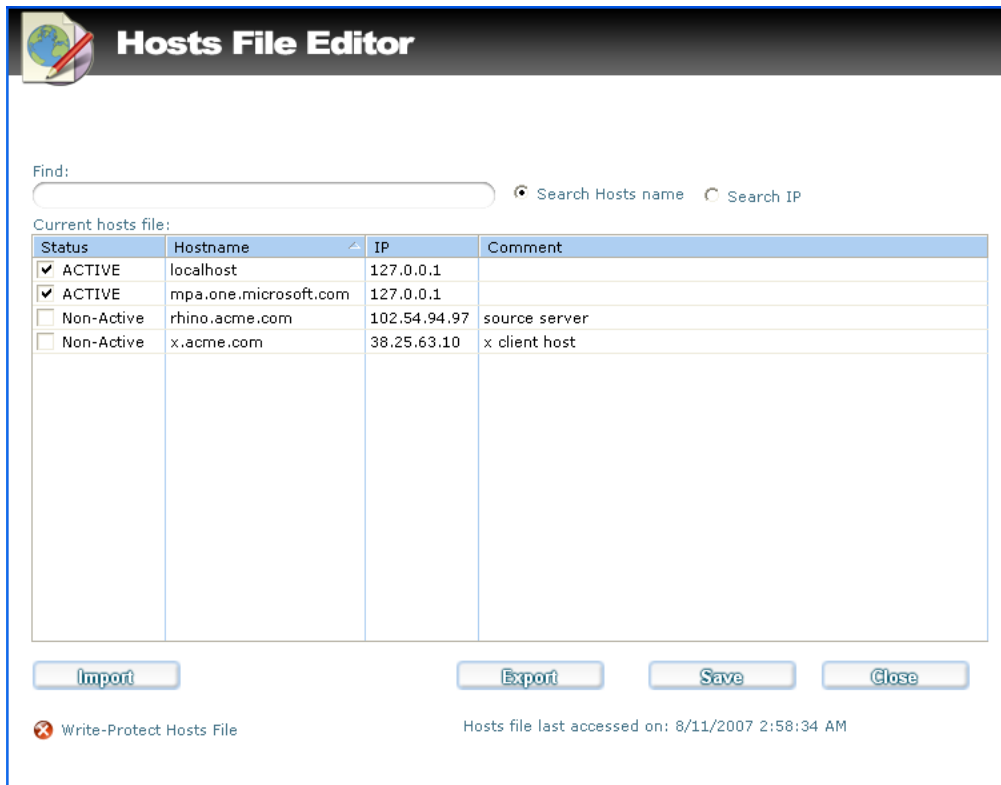
Using Hosts File Editor

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 "Find" field allows you to search through your current Host File for a specific IP address or Host name.

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." Check the box to change the status of the selected host name to active or non-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.

Click "Import" to import other Host File entries info the Hosts File Editor.

Click "Export" to save your Hosts File as a text file.

Click "Save" to save the changes you made.

Click "Close" to close the Host File Editor.

Check the box beside "Write-Protect Host File" to Write protect your Hosts File so that it cannot be altered by other programs.

AutoStart Manager

The AutoStart Manager is a powerful tool that lets you choose what programs and services are allowed to start automatically when Windows loads.
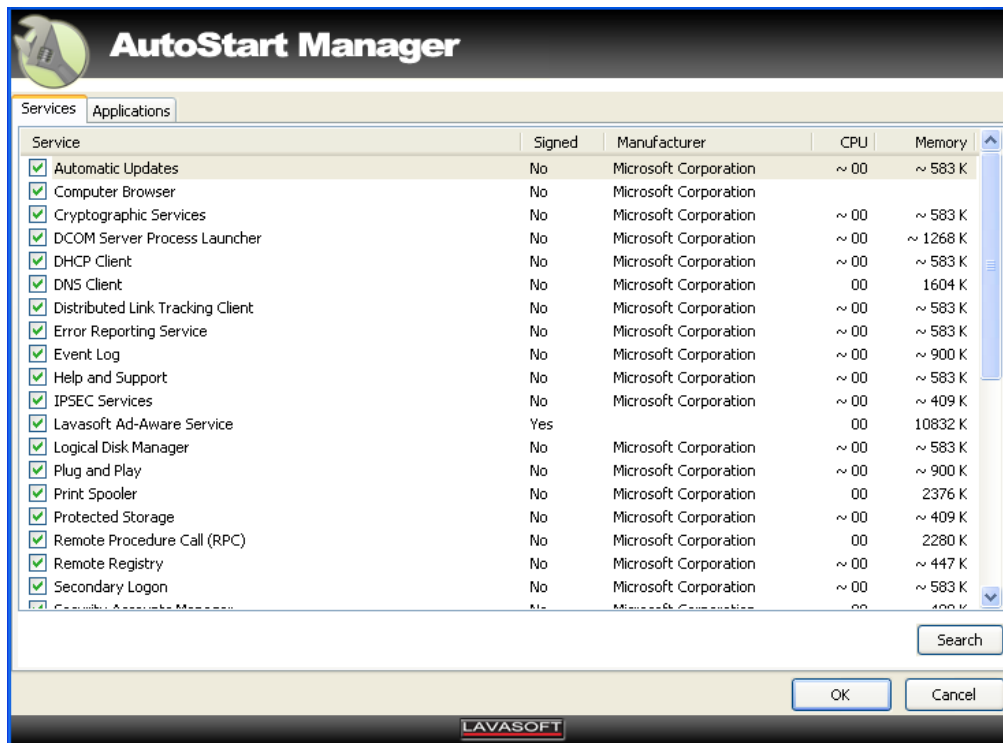
Using AutoStart Manager

When the AutoStart Manager is launched, it shows you a list of all the running services in the services tab.

In the Applications tab, you can see a list of all the running services/processes on your system that start automatically.

The services and Autorun windows list information by:

- **Service:** Lists the file name of the service running on your system.
- **Signed:** Shows if the service is signed or not. A signed service has a digital signature added by its manufacturer.
- **Manufacturer:** Shows the manufacturer that has created this service.
- **CPU:** Shows the CPU usage of that service.
- **Memory:** Shows the amount of memory used by the process.

AutoStart Manager Context Menu

Right-clicking on the AutoStart Manager window opens the context menu, showing the operations you can perform on any given service.

You can choose from the following operations:

- **Disable:** Disables the selected service.
- **Info:** Opens a new window showing the process/service properties.
- **Search:** Brings you directly to a Google search to access more information about the selected service.

ThreatWork

ThreatWork gives you direct access to submit suspicious files for analysis via an alliance of global anti-spyware security volunteers, protecting personal computers and business networks worldwide. Submit your suspicious files today and become a valuable contributor to Lavasoft ThreatWork.

To open Threatwork, click "Toolbox" in the sub-menu and "Start" under the ThreatWork heading. You can also open ThreatWork from the Windows start menu.

From the ThreatWork window, you can submit files by either dragging and dropping files for submission, or by selecting items using the "Browse" button.

You can configure ThreatWork's settings in the update settings.

Settings

Updates

Configure the updates settings for the software & Definitions File, information updates, Threatwork and proxy settings.
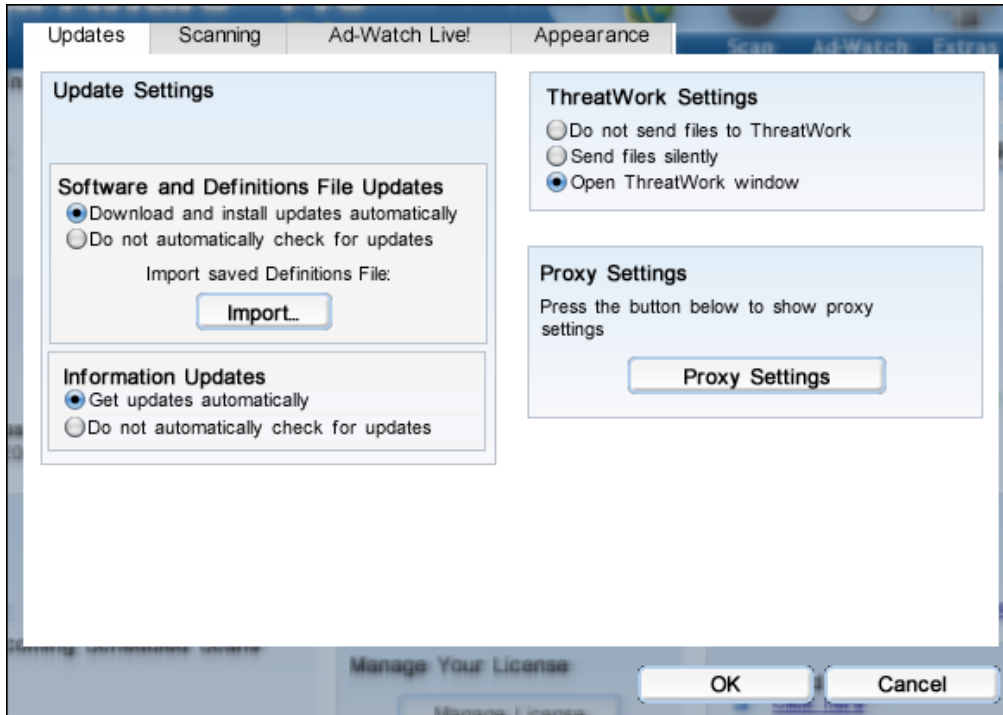
Update Settings

Important: Absolutely no confidential information will be collected that could identify you, your location, or anything else that might compromise your privacy while performing an update. Please visit our website for more information regarding Lavasoft's Privacy Policy.

Software and Definitions File Updates

You can adjust the software to automatically download and install Definitions File and software updates.

When a new update is available, it will automatically be downloaded to your computer.

You can also save the Definitions File to a specific location on you computer by clicking the "Import" button.

Information Updates

You can adjust the information updates to keep informed and updated about Lavasoft (company information, industry news, etc.) This is automatically displayed in the main status window.
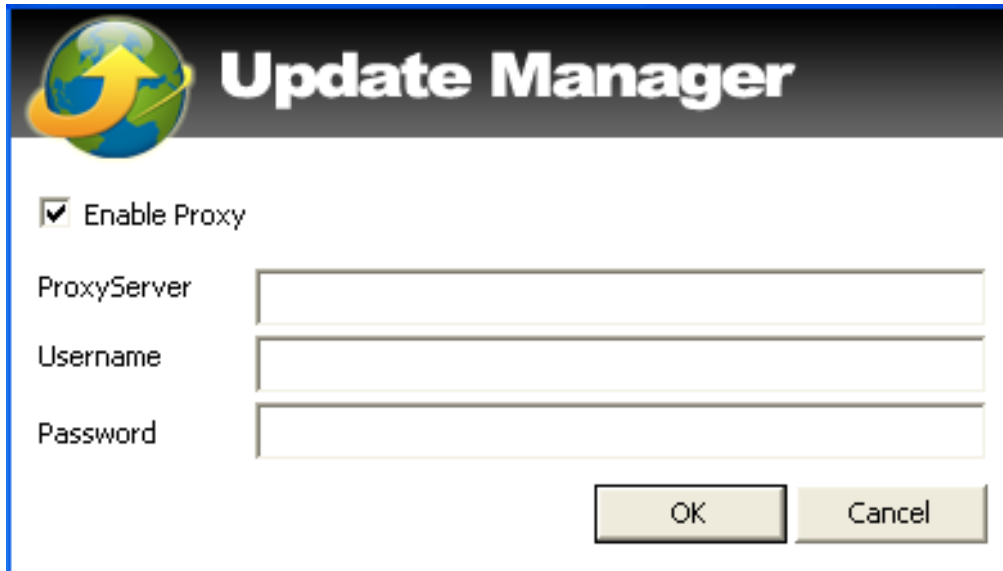
ThreatWork Settings

You can configure ThreatWork to automatically submit suspicious files silently (meaning you do not see the ThreatWork window), or to open the ThreatWork window when sending files. You can also turn this setting off.

We do, however, recommend that you have this option turned on to submit your suspicious files and become a valuable contributor to Lavasoft ThreatWork

Proxy Settings

If you are operating behind a proxy server, you will need to have your proxy server settings correctly configured in order to perform updates.

Click the "Proxy Settings" button to configure the proxy server settings.

To Enable tick the box beside "Enable Proxy", enter your proxy server address, your username and password and click 'Ok'.
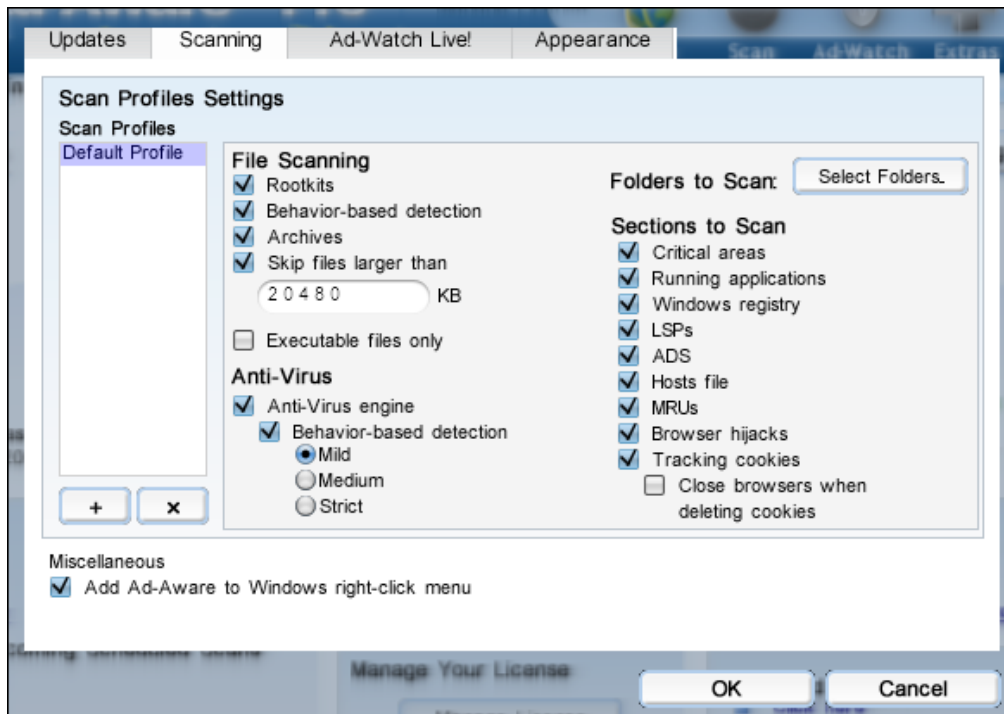
To Disable untick the "Enable Proxy" box and click "Ok".

Click "Ok" to apply any changes made.

Click "Cancel" to cancel any changes made and to close the settings window.

Scanning

Configure the profile scanning settings.

Scan Profiles

Choose which profile to use/edit from the list. Click "+" to add a new profile. To delete a profile click "x".

File Scanning

Rootkits: A method of hiding files or processes from normal methods of monitoring. This technique is often used by malware to hide its presence and activities.

Spyware Heuristics: Scans with behavior-based detection. A method of detecting unknown malware using systems of rules and patterns.

Archives: Scans within archives such as .zip and .rar .

Executable files only: Scans only for executable files - files with the extension .exe

Skip files larger than: The scan 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.

Folders to Scan

Select specific folders on your computer to scan by clicking the "Selected Folders" button.

Sections to Scan

Application starting points: Scans applications that are configured to start automatically.

Running applications: Refers to applications that are active in memory.

Windows registry: Scans known spyware areas of the registry.

Layered Service Providers (LSP's): Detects and unloads malicious LSP's. LSP's are used by malicious software to detect network activity. The LSP's must be loaded for Ad-Aware to detect them.

Alternate Data Stream (ADS): Scans files and simultaneously investigates ADS streams for malicious objects.

Host 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.

Most Recently Used (MRUs): A link to a recently opened file, document or program.

Browser hijacks: Scans browser settings (like start page and search page), favorites, and desktop for malicious URLs.

Tracking cookies: A tracking cookie is any cookie used to track a user's surfing habits. They are typically used by advertisers wishing to analyze and manage advertising data, but they may be used to profile and track user activity more closely. However, tracking cookies are simply a text file, and a record of visits or activity with a single website or its affiliated sites.

Close browsers when deleting cookies: When this option is selected, any open browser will be automatically closed when deleting cookies.

Anti-Virus
Anti-virus engine: Check this box to use Ad-Aware's extended anti-virus scanner.

If you choose to scan using behavior-based detection, select the level of Heuristics to be used.
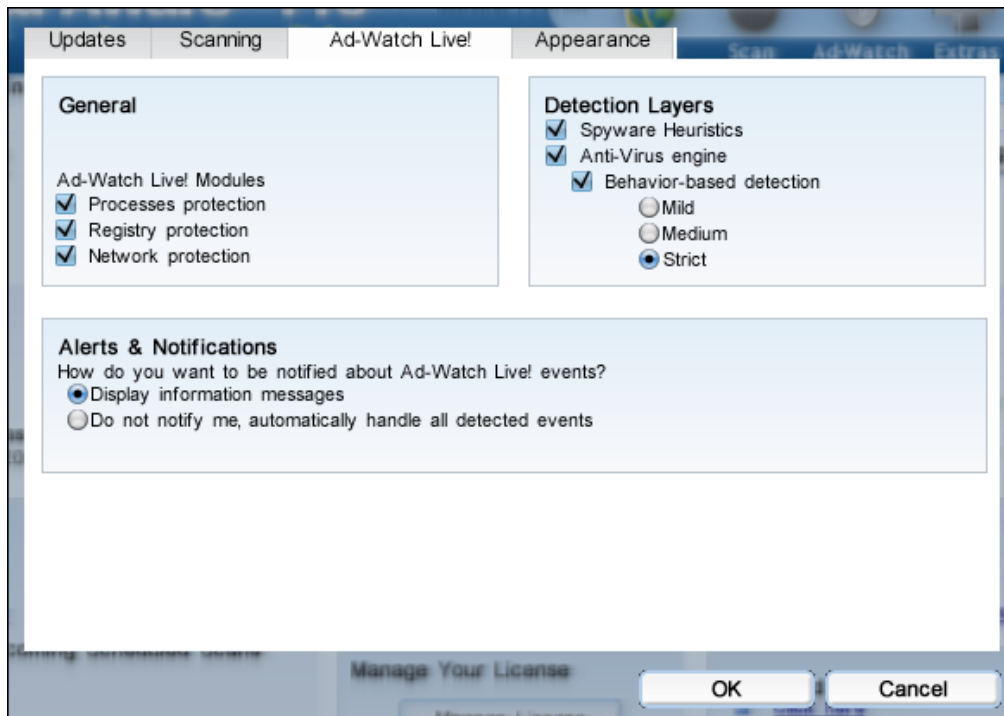
Miscellaneous
Add Ad-Aware to Windows right-click menu: This setting allows you to use the right-click menu to scan a file or folder with Ad-Aware.

Click "Ok" to apply any changes made.

Click "Cancel" to cancel any changes made and to close the settings window.

Ad-Watch Live

Configure the Ad-Watch Live! settings.

General
Ad-Watch Live! modules: Choose which Ad-Watch Live! modules to have on or off.

Detection Layers
Spyware Heuristics: Files are analyzed with behavior-based detection. A method of detecting unknown malware using systems of rules and patterns.

Anti-virus engine: Check this box to use Ad-Aware's extended anti-virus scanner.

If you choose to scan using behavior-based detection, select the level to be used.

Alerts & Notifications
Choose how you want to be notified about Ad-Watch Live! events.

Display information messages: All information messages are displayed in the tray icon.
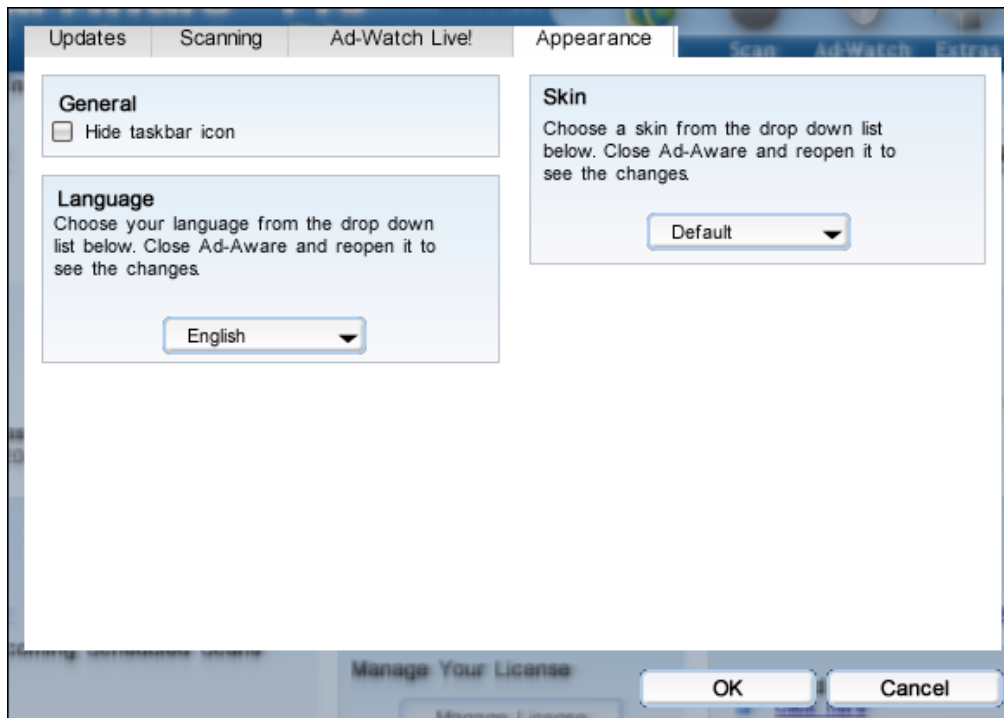
Do not notify me, automatically handle all detected events: Events are automatically handled and no Ad-Watch notification will appear in the system tray.

Click "Ok" to apply any changes made.

Click "Cancel" to cancel any changes made and to close the settings window.

Appearance

Configure the appearance and choose your preferred language of Ad-Aware.

General
Hide taskbar icon: When selected the Ad-Aware icon will not appear in the system tray.

Language
Choose your preferred language from the drop-down list and click "Ok" to change the language.

Restart Ad-Aware to view the program in your preferred language.

Skin
You can change the look of the program by changing skins.

Choose a skin from the drop-down list and click "Ok" to the change the appearance of Ad-Aware.

Click "Ok" to apply any changes made.

Click "Cancel" to cancel any changes made and to close the settings window.

Tray Application

Right click on the Ad-Aware Tray Application in the system tray (the bottom right menu beside the clock).

Double-clicking on the Tray Application gives you fast access to Ad-Aware's main user interface. It also includes the options shown below.

Open Ad-Aware
Opens the Ad-Aware program.

Open ThreatWork
Gives you direct access to submit suspicious files for analysis via ThreatWork.

Disable/Enable Ad-Watch Live!
Disables/Enables Ad-Watch Live! real-time protection. This temporally disables Ad-Watch Live!

To fully disable Ad-Watch Live!, please go to the Ad-Watch Live! settings.

Run Scan
From the sub-menu, you can choose to run a Smart, Full or Profile scan.

Run Update
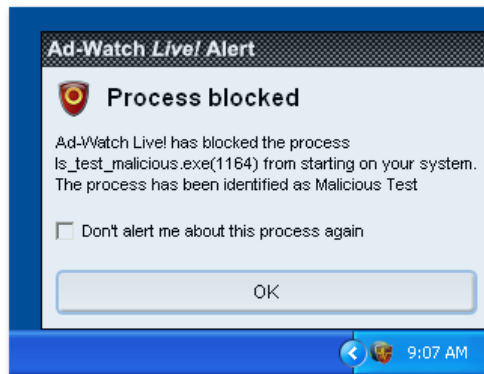Downloads and installs any available updates.

Exit Ad-Aware
Exits the Ad-Aware program completely.

Notifications

Process Notification

Ad-Watch Live! Process Notification

When any malicious process starts on your computer, this Ad-Watch Live! notification window will appear. Tick the box beside "Don't alert me about this process again" and no Ad-Watch notification will appear the next time this process starts.

When any suspicious process starts on your computer, this Ad-Watch Live! notification window will appear.

Click 'Allow' and the process will be allowed to run. Warning! Only use this action if you are sure that the process is safe.

Click 'Block' and the process will be blocked from running.

For each process, you can change the 'Action' as described in the Process Rules section.

Ad-Watch Live! Registry Notification

When any application makes a change your computer's registry, this Ad-Watch Live! notification window will appear and you will be given the choice to 'Allow' or 'Block' this registry change. Click 'Allow' and the process will be allowed to run. Warning! Only use this action if you are sure that the process is safe.

Click 'Block' and the process will be blocked from running.

Tick the box beside "Remember my choice and do not alert for this process again", for Ad-Watch Live! to remember your choice.

For each registry change, you can choose the 'Action' as described in the Registry Rules section.

Ad-Watch Live! Network Notification
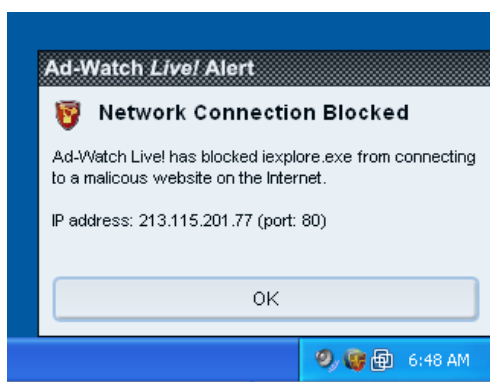
When any application tries to connect to a blacklisted IP address that is detected as malicious, the Ad-Watch notification window will inform you that it was blocked. For each connection to a blacklisted IP address, you can change the 'Action' as described in the Network Rules section.

Click "Ok" to close the notification window.

Using Command Line Parameters

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

Example:

```
C:\Program Files\Lavasoft\Ad-Aware>Ad-Awarecommand.exe scan full
```

Ad-Aware will run in the background (without the GUI) and perform a Full Scan with automatic cleaning.

Scanning Parameters

```
scan smart
```

This parameter will run a Smart system scan with automatic cleaning.

```
scan full
```

This parameter will run a Full system scan with automatic cleaning.

```
scan Profile name
```

This parameter will run a user-defined profile scan with automatic cleaning.

Replace 'Profile name' with the actual scan profile name. If there is a space in the Profile name you must include double quotes, eg "My Scan Profile."

If the Profile name doesn't exist a list of the existing Profile names are shown.

```
manual
```

This is an optional parameter used when you want to manually choose the cleaning actions.

When you use this parameter the scan will run silently and when its completed the Tray Application will notify you that the scan is finished. From the Tray Application open the scan results screen to manually choose the required action for each detected object.

Updates

```
update all
```

This parameter performs both definition and software updates if available.

```
silent
```

This is an optional parameter used to suppress the dialog during an update.

Uninstall Ad-Aware

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

Uninstaller
1. Go to the "Lavasoft\Ad-Aware" folder in your Start menu.
2. Run "Uninstall Ad-Aware."
3. Verify uninstalling by selecting "Uninstall."
4. Your computer must be restarted to completely unload and remove all Ad-Aware files/folders. Click the option to "Restart Now" and click "Finish" to complete the uninstall process. We kindly ask you to complete the "Feedback" option to help us improve our software.
5. When the computer restarts, Ad-Aware will be fully uninstalled.

Control Panel
1. Go to the Control Panel.
2. Run "Add or Remove Programs".
3. Select Ad-Aware in the list and click the "Remove" button.
4. Verify uninstalling by selecting "Uninstall."
5. Your computer must be restarted to completely unload and remove all Ad-Aware files/folders. Click the option to "Restart Now" and click "Finish" to complete the uninstall process. We kindly ask you to complete the "Feedback" option to help us improve our software.
6. When the computer restarts, Ad-Aware will be fully uninstalled.