LAVASOFT

Ad-Aware®

User Manual

Table of Contents

Ad-Aware Overview

Getting Started

Using Ad-Aware

Ad-Aware Overview

What Is Ad-Aware?

Ad-Aware is Lavasoft's industry leading Internet security solution that allows you to combat stealthy online threats and the latest advancements by cyber criminals. Ad-Aware protects you from 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.

With minimal strain on system resources, additional usability features for added control, and power-packed advancements to our anti-malware technology, including advanced Genotype detection technology and a deep level rootkit removal system, Ad-Aware gives all users the power to protect their privacy and security online. Hand in hand with this release, Lavasoft has also introduced new community-based initiatives that give even more power to the people, including community-driven translations, product skins, and plug-ins, as well as the opportunity for more user interaction through the MyLavasoft community.

Ad-Aware is available in the following versions:

Ad-Aware Free Anti-Malware
anti-spyware + anti-rootkit

Ad-Aware Plus Internet Security
anti-virus + anti-spyware + anti-rootkit

Ad-Aware Pro Internet Security
anti-virus + anti-spyware + anti-rootkit

Ad-Aware Free is a proactive malware removal tool with real-time protection against spyware, Trojans, rootkits, hijackers, keyloggers, and more. The Plus and Pro versions boost security with full virus protection, including behavior-based heuristics scanning, expert rootkit removal technology, and other premium features.

Ad-Aware Features

Smart defense against advanced threats

- **Comprehensive malware protection -** Powerful protection against spyware, trojans, worms, malware, rootkits, rogue applications and much more. **(*Free, Plus, Pro*)**
- **Anti-Virus -** Detection, removal, and repair of traditional virus threats. **(*Plus, Pro*)**
- **Ad-Watch *Live!* Basic -** Real-time process protection blocks malicious processes and infected programs that try to start or run on your system. **(*Free, Plus, Pro*)**
- **Ad-Watch *Live!* Advanced -** Real-time registry protection and process protection including behavior-based heuristics scanning. **(*Plus, Pro*)**
- **Ad-Watch *Live!* Expert -** Gives you an additional layer of security by blocking connections to blacklisted IP addresses. It also adds real-time network protection, registry protection, and process protection including behavior-based heuristics scanning. **(*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. **(*Free, Plus, Pro*)**
- **Genotype Detection Technology -** Based on heuristics, Genotype allows Ad-Aware to stay one step ahead of today's ever-evolving threats, as well as threats that have not yet been created. For in-depth information on this technology, please click here. **(*Free, Plus, Pro*)**
- **Rootkit Removal System -** Protection against hidden threats and stealth attacks. **(*Free, Plus, Pro*)**
- **The Neutralizer -** Advanced removal tool combats malware that attempts to restore itself even after rebooting your system. **(*Free, Plus, Pro*)**
- **Download Guard for Internet Explorer-** Provides an additional layer of protection that lets you download files on Internet Explorer confidently. **(*Free, Plus, Pro*)**

Your online safety net

- **Detect, remove *AND* repair -** Ad-Aware intelligently cleans your system by removing all traces of the infection. **(*Free, Plus, Pro*)**
- **External Drive Scanning -** Scan your external storage device, iPod, USB’s, or any other drives that you connect to your PC for an additional layer of security. **(*Free, Plus, Pro*)**
- **Network Drive Scanning -** Scan network drives so you can detect malware on any shared disks on your network. **(*Pro*)**
- **Pin-Point Scanning -** Right click any file or folder to perform an immediate scan to determine if it's safe or not. **(*Free, Plus, Pro*)**
- **System Restore Point -** Set a system restore point so you can clean your PC without fear of obstructing your operating system. **(*Free, Plus, Pro*)**

Features to simplify your life

- **Minimal use of computer resources. (*Free, Plus, Pro*)**
- **Do Not Disturb Mode -** Stay protected while watching videos, playing games, or making presentations in full screen mode - without annoying interruptions or strain on system resources that other security software programs cause. **(*Pro*)**
- **Customizable Profile Scans -** Save time by creating profile scans for even faster, more efficient scans. **(*Free, Plus, Pro*)**
- **Lavasoft SmartSet -** Based on expert recommended settings, we have configured your Ad-Aware to make scanning and cleaning your computer as easy as possible. **(*Free, Plus, Pro*)**
- **Simple Mode / Advanced Mode -** Simple Mode is designed to make using the program as easy as possible, whereas Advanced Mode will let you customize all the settings as you

choose. (***Free, Plus*, *Pro***)

- **Automatic Updates -** Continuous pulse updates to guard your privacy against cyber attacks throughout the license duration. (***Free, Plus*, *Pro***)
- **Full Integration with Windows Security Center -** Get Ad-Aware protection and status notifications through the Windows Security Center, if for example, any part of your security has been turned off or disabled. (***Free, Plus*, *Pro***)
- **The Scheduler -** Automatic Scans set to your personalized schedule to optimize time and resources. If used in combination with Lavasoft SmartSet, all you have to do set & forget. (***Plus*, *Pro***)
- **Free Technical Support -** Direct, in-product access to the Lavasoft Support Center. (***Plus*, *Pro***)

Bonus tools for an additional layer of security

- **Lavasoft Toolbox -** Block unsecure and harmful websites with the Hosts File Editor; keep track of all running processes with Process Watch; reduce the toll on your system with the AutoStart Manager, and submit suspicious files to ThreatWork Alliance. (***Pro***)
- **Command Line Support -** Manage Ad-Aware without launching the interface window. (***Pro***)
- **Lavasoft ThreatWork Alliance -** ThreatWork Alliance allows us to provide the best protection possible against the newest and most relevant threats, through the help of our community of security volunteers. (***Free, Plus*, *Pro***)
- **TrackSweep -** Control your privacy by erasing tracks left behind while surfing the web. (***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***)
- **Community-Driven Skins -** We now give you the power to control the look of Ad-Aware. Pick a new look in our Skin Gallery or design your very own skin. The power is in your hands! (***Free, Plus*, *Pro***)
- **Community-Driven Translations -** This is the people's product, so the new XML-based language format of the GUI allows you to edit and upload translated text to share with the world. Power to the people! (***Free, Plus*, *Pro***)

System Requirements

When installing Ad-Aware on Windows 2000, XP, Vista and Windows 7 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 7, Windows Vista (32- and 64-bit), Windows XP (32-bit), Windows 2000 Pro.

Getting Started

Install Ad-Aware

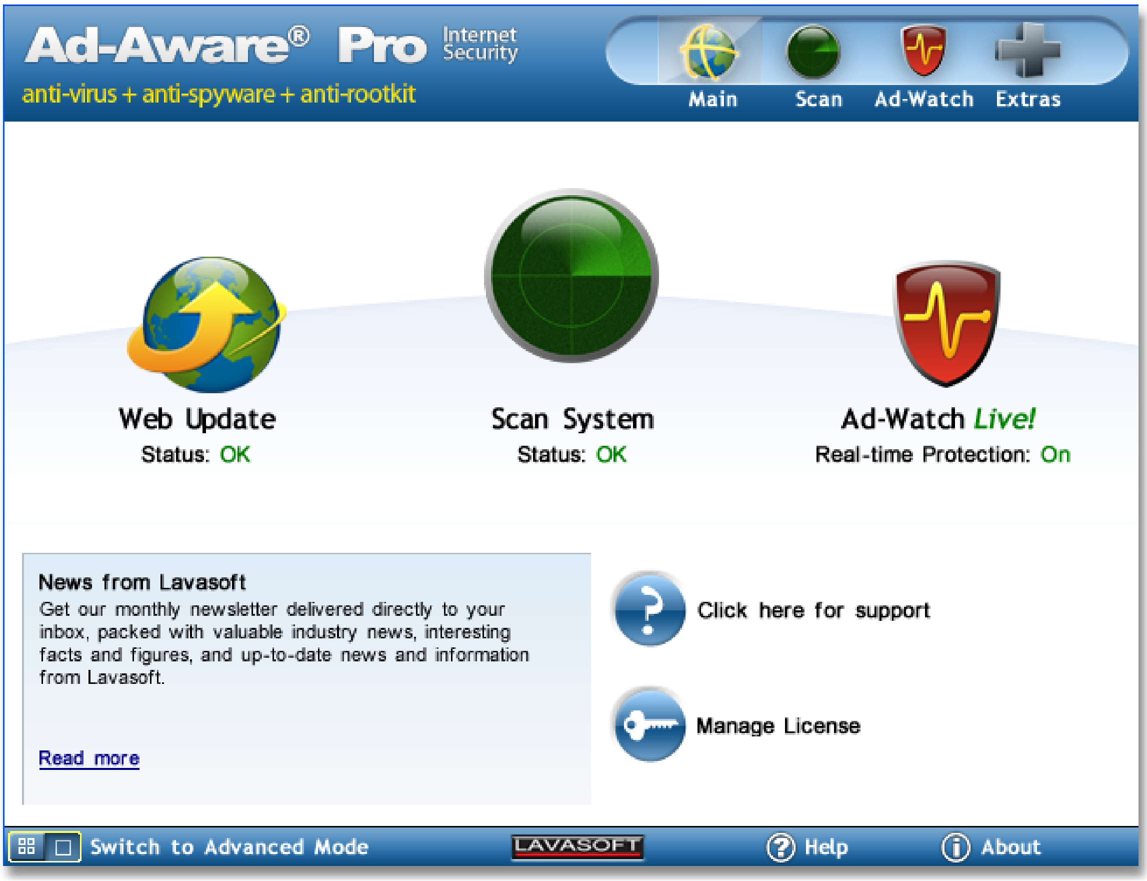
- **Start Installation**
  If you are installing Ad-Aware from a CD, insert the CD into the CD-ROM drive. If you downloaded your copy of Ad-Aware, locate and double-click on the downloaded file to start the installation.
- **Language Selection Window**
  Choose your preferred language and click "Ok."
- **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", and click “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.”
  - Choose to install/don’t install Ad-Watch *Live!* and Download Guard for Internet Explorer by ticking/unticking these options.

  Click ‘’Ad-Aware only’’ or ‘’Install Ad-Aware and Google Chrome’’. Click "Install" to continue with the 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. By default the option to "Restart now" is ticked. Untick this to restart later. 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.

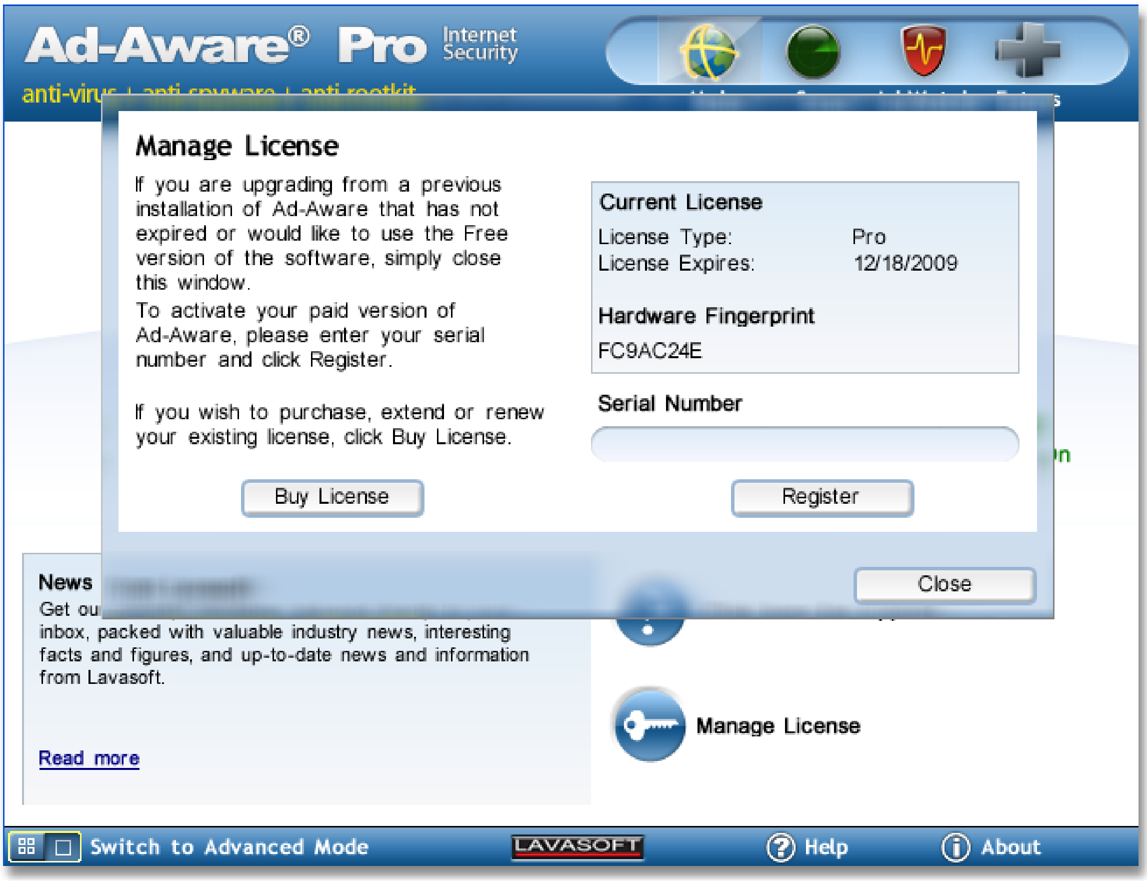


News from Lavasoft
Get our monthly newsletter delivered directly to your inbox, packed with valuable industry news, interesting facts and figures, and up-to-date news and information from Lavasoft.

Read more

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.



Manage License

If you are upgrading from a previous installation of Ad-Aware that has not expired or would like to use the Free version of the software, simply close this window.

To activate your paid version of Ad-Aware, please enter your serial number and click Register.

If you wish to purchase, extend or renew your existing license, click Buy License.

Current License

License Type:	Pro
License Expires:	12/18/2009

Hardware Fingerprint

FC9AC24E

Serial Number

Ad-Aware® Pro Internet Security
anti-virus | anti-spyware | anti-rootkit
Buy License
Register
Close
News
Get ou… inbox, packed with valuable industry news, interesting facts and figures, and up-to-date news and information from Lavasoft.
Read more
Manage License
Switch to Advanced Mode
LAVASOFT
Help
About

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 log-in to the Lavasoft Support Center by clicking here, and click the ‘reset serial’ button located just below your serial number in the ‘My Licenses’ section. Once the serial is 'reset' you will be able to reactivate Ad-Aware.

If you do not have a serial key or your license has expired and you 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. If your license has expired and you want to continue using the free version, please uninstall Ad-Aware, then download and install Ad-Aware Free from www.lavasoft.com.

Using Ad-Aware

We know that not all users have the same needs; that's why Ad-Aware has two modes that allow you to decide how you want to interact with the program: Simple Mode and Advanced Mode.

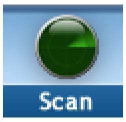
On first installation, Simple Mode starts by default. To switch between Simple and Advanced Modes, click the icon at the bottom left of the screen.

Opens Ad-Aware in Advanced Mode.

Opens Ad-Aware in Simple Mode.

Main Menu Buttons

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. 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.

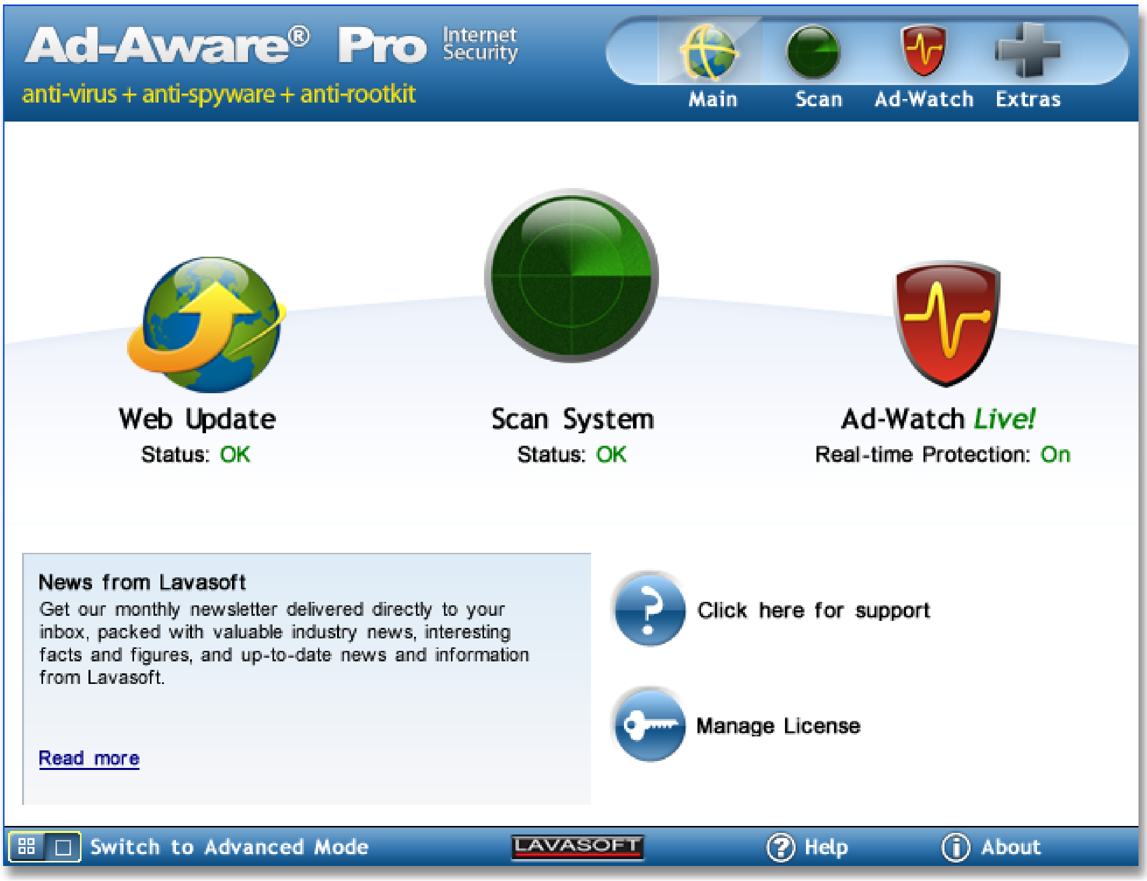
Opens the Ad-Aware product manual.

Opens copyright and contributor information about Ad-Aware.

Main

Simple Mode is designed to make using the program as easy as possible, allowing you to “set and forget” by using our expert recommended settings.

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



News from Lavasoft

Get our monthly newsletter delivered directly to your inbox, packed with valuable industry news, interesting facts and figures, and up-to-date news and information from Lavasoft.

Read more

The Main screen displays a simple 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!* status , view the latest industry news, contact our Support Team (Plus and Pro versions) and manage your license.

Click “Web Update”, the Update Manager will open, then download and install any available updates. The software is automatically updated for your convenience.

Click the "Scan System" icon to run a system scan. The scan is started directly and detected objects are automatically handled by using our expert recommended settings. A smart scan is started if a scan has already being run within the last four days, otherwise a full scan starts.

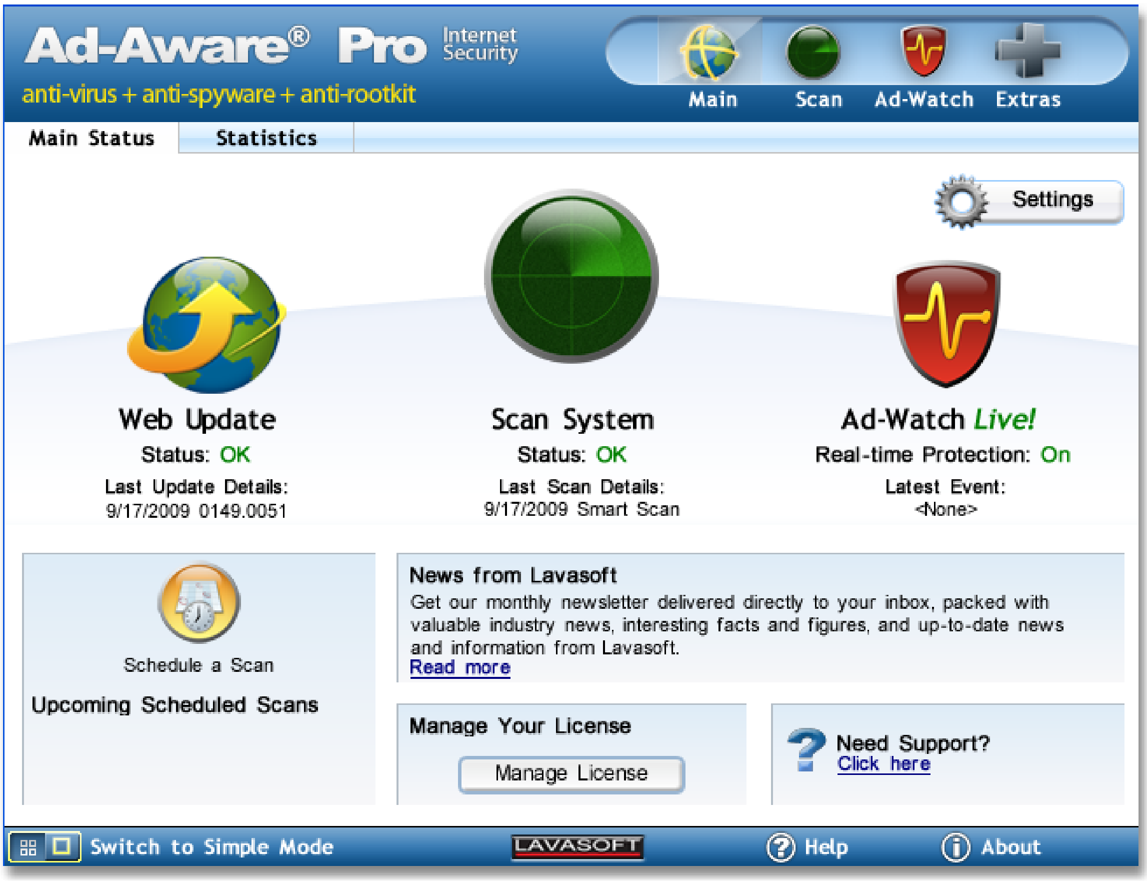
Click the "Ad-Watch *Live!*" icon to open the Ad-Watch Live! real-time protection screen.

Click to switch to Advanced Mode, to customize all the settings.

Main Status

Advanced Mode will let you customize all the settings as you choose, to tailor everything to your specific needs.

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, view the latest industry news and manage your license. For the Plus and Pro versions you can also schedule scans and contact our Support Team with technical inquiries.



Ad-Aware® Pro Internet Security
anti-virus + anti-spyware + anti-rootkit
Main
Scan
Ad-Watch
Extras
Main Status
Statistics
Settings

Web Update
Status: OK
Last Update Details:
9/17/2009 0149.0051

Scan System
Status: OK
Last Scan Details:
9/17/2009 Smart Scan

Ad-Watch *Live!*
Real-time Protection: On
Latest Event:
<None>

Schedule a Scan
Upcoming Scheduled Scans

News from Lavasoft
Get our monthly newsletter delivered directly to your inbox, packed with valuable industry news, interesting facts and figures, and up-to-date news and information from Lavasoft.
Read more

Manage Your License
Manage License

Need Support?
Click here

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 ensure to have the latest updates by performing a Web Update. You can configure the way Ad-Aware handles 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.

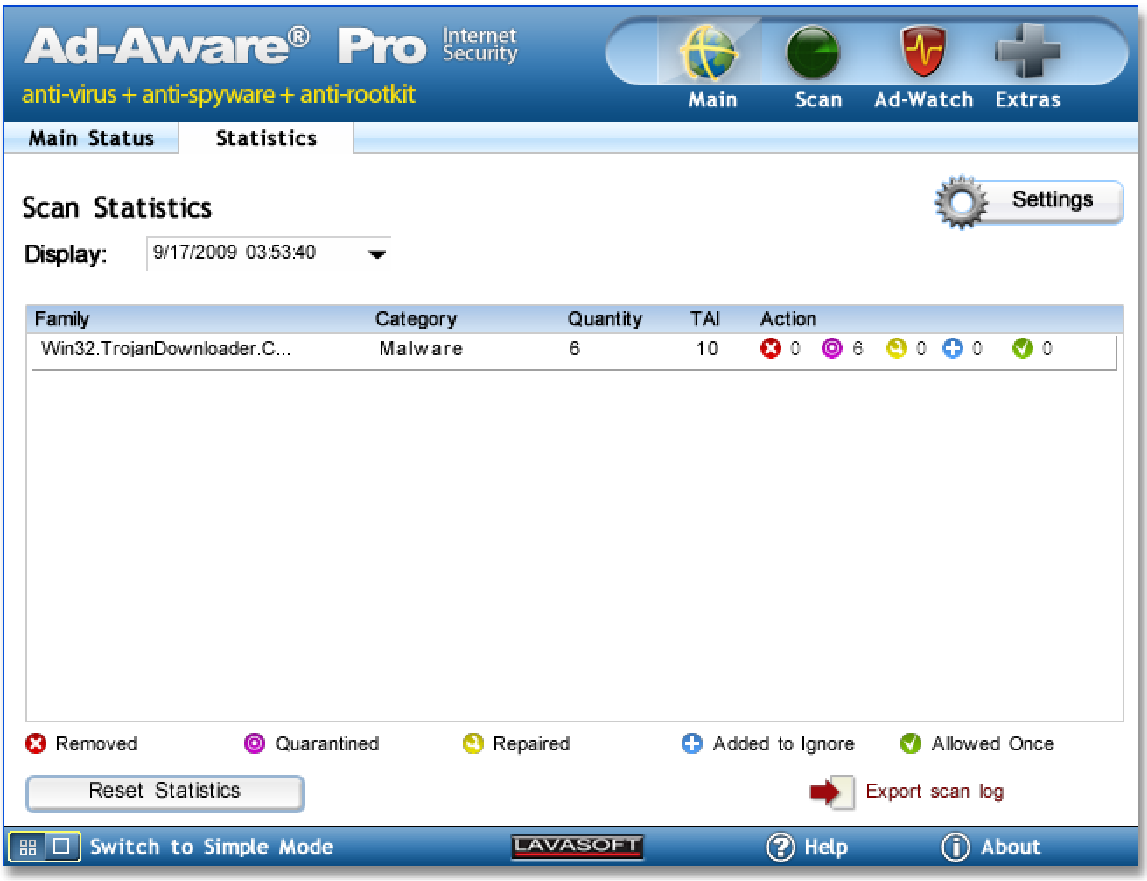
Click "Settings" to open the Settings screen where you can customize Ad-Aware to fit your needs.
The settings are context sensitive, meaning that when you click on settings for

a particular feature, the settings for that feature open. Use the tabs in the sub-menu to navigate between different categories of settings.

Switch to Advanced Mode	Opens Ad-Aware in Advanced Mode.
Switch to Simple Mode	Opens Ad-Aware in Simple Mode.

Statistics

Shows statistics about the objects detected in previous scans.



Scan Statistics

Display: 9/17/2009 03:53:40

Family	Category	Quantity	TAI	Action
Win32.TrojanDownloader.C...	Malware	6	10	✖ 0 ◎ 6 ● 0 ✚ 0 ✓ 0

✖ Removed ◎ Quarantined ● Repaired ✚ Added to Ignore ✓ Allowed Once

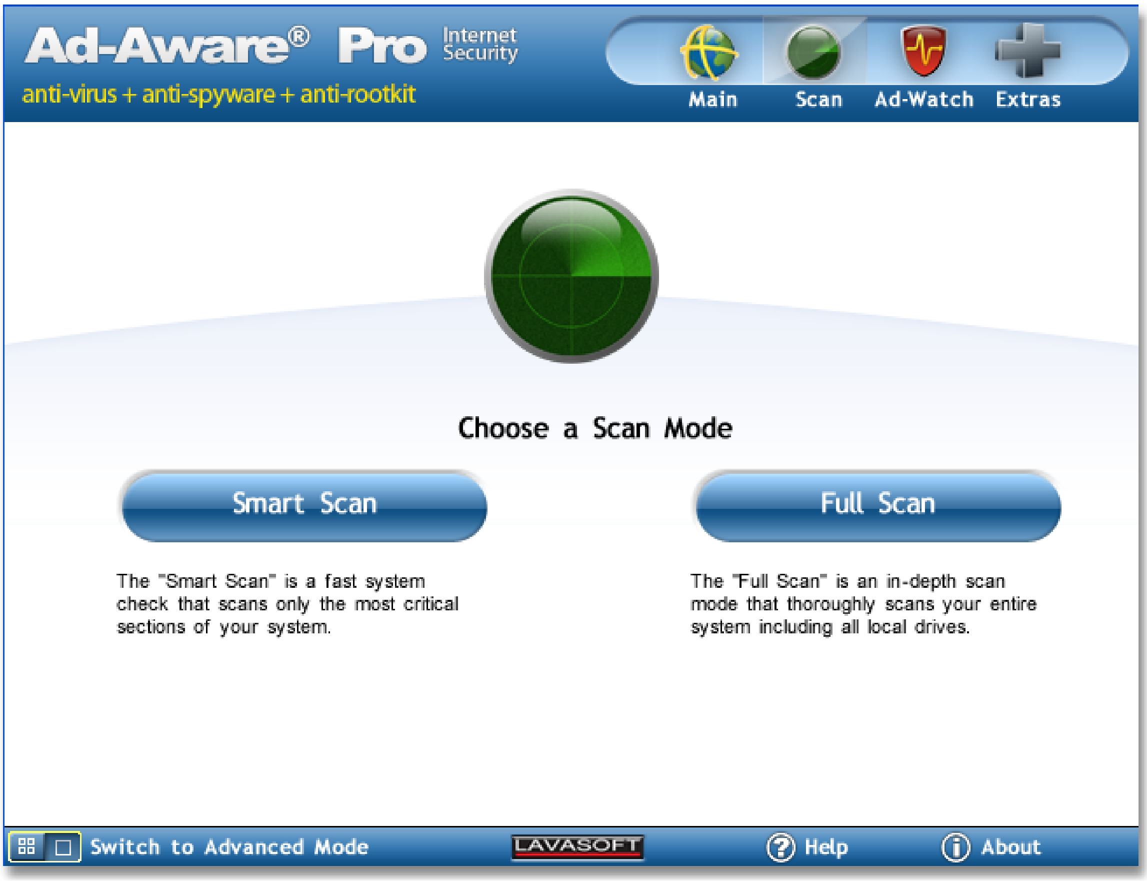
Choose “Statistics” from the “Display” drop-down menu.
You can choose to display the total or the statistics from a specific time.
Once selected, the “Scan Statistics” table will refresh.
The statistics from a scan run within Simple Mode will also be available in the drop-down menu.

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

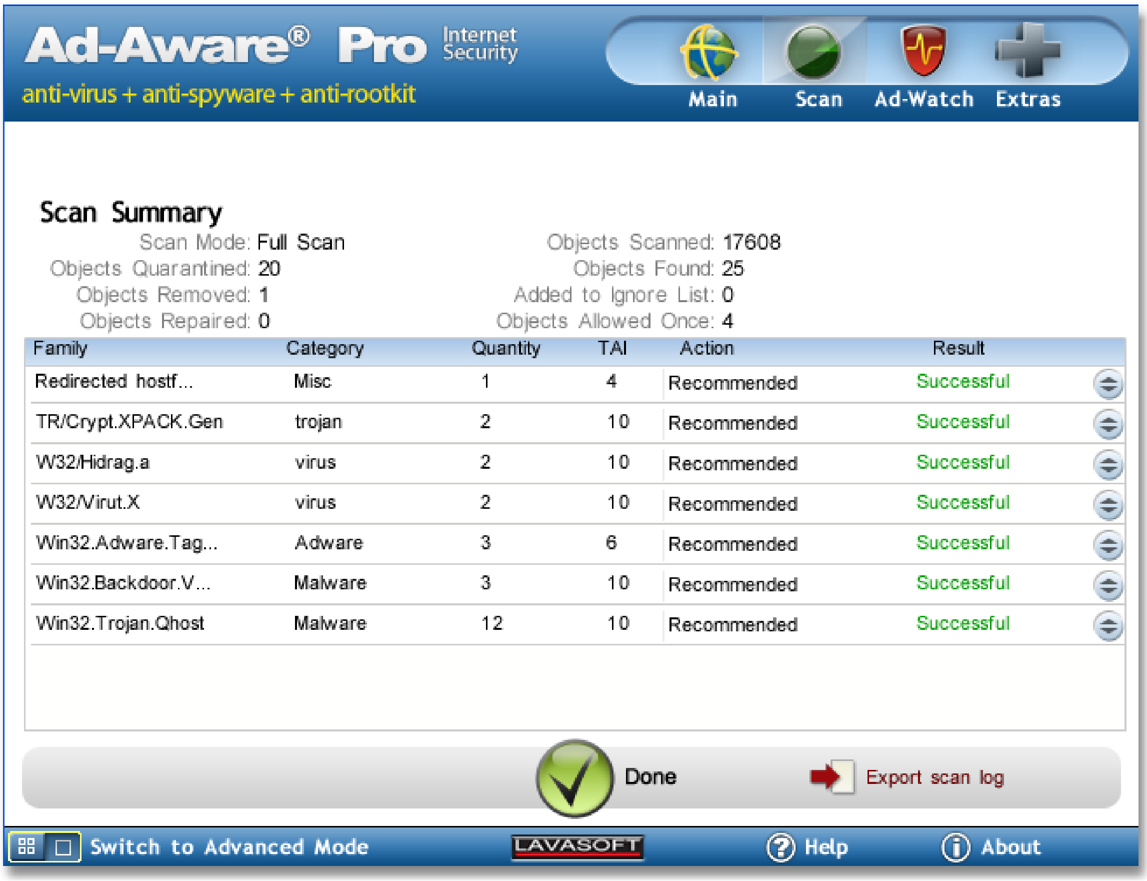
Click the “Scan” menu button to open the “Scan Mode” screen, where you can choose the type of scan you would like to perform - a Smart Scan or a Full Scan.



The "Smart Scan" is a fast system check that scans only the most critical sections of your system.

The "Full Scan" is an in-depth scan mode that thoroughly scans your entire system including all local drives.

Once the scan is completed, detected objects are automatically handled by using our expert recommended settings. The Scan Summary screen shows information about the scan that you performed.
Once you have reviewed the scan results, click "Done" to close this screen.


Ad-Aware® Pro Internet Security
anti-virus + anti-spyware + anti-rootkit
Main
Scan
Ad-Watch
Extras

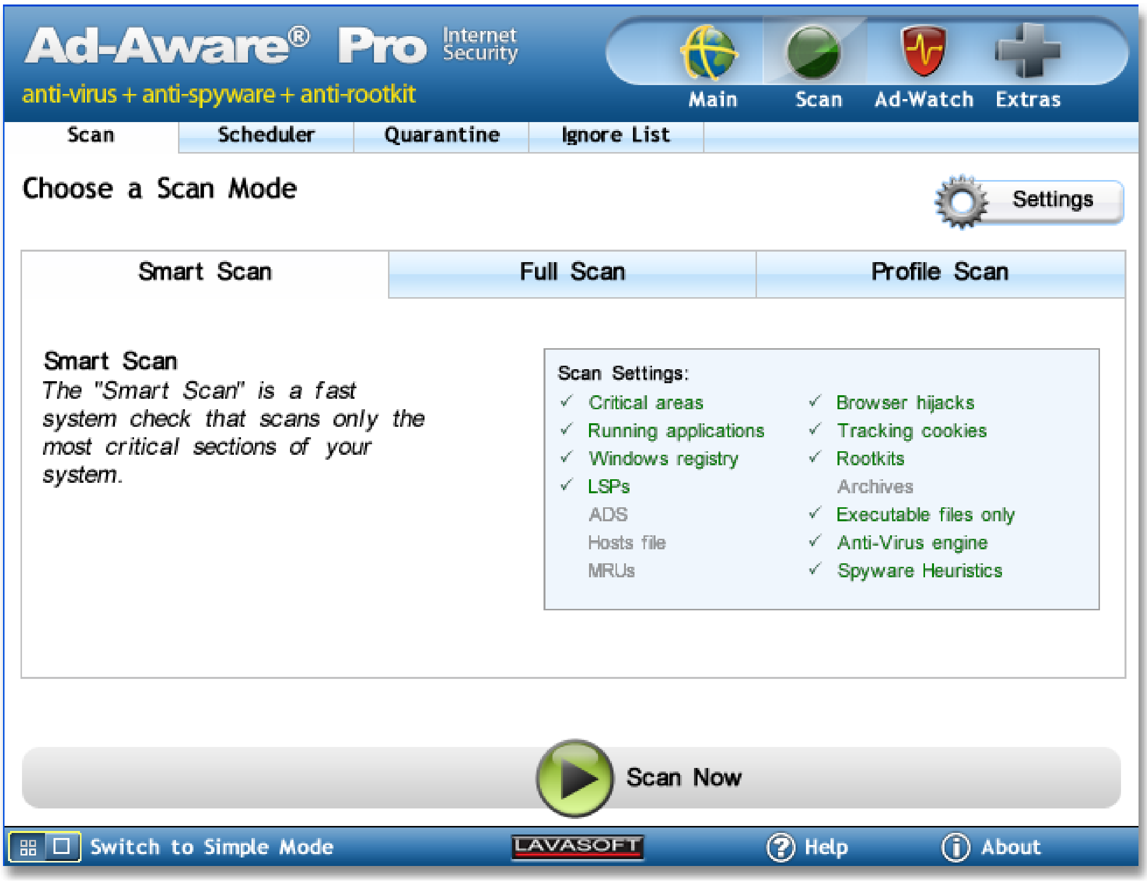
Scan Summary

Scan Mode: Full Scan
Objects Quarantined: 20
Objects Removed: 1
Objects Repaired: 0
Objects Scanned: 17608
Objects Found: 25
Added to Ignore List: 0
Objects Allowed Once: 4

Family	Category	Quantity	TAI	Action	Result
Redirected hostf...	Misc	1	4	Recommended	Successful
TR/Crypt.XPACK.Gen	trojan	2	10	Recommended	Successful
W32/Hidrag.a	virus	2	10	Recommended	Successful
W32/Virut.X	virus	2	10	Recommended	Successful
Win32.Adware.Tag...	Adware	3	6	Recommended	Successful
Win32.Backdoor.V...	Malware	3	10	Recommended	Successful
Win32.Trojan.Qhost	Malware	12	10	Recommended	Successful

Switch to Advanced Mode: Click to switch to Advanced Mode, to customize all the settings.

Choose A Scan Mode



Choose a Scan Mode

Smart Scan
The "Smart Scan" is a fast system check that scans only the most critical sections of your system.

Scan Settings:

- ✓ Critical areas
- ✓ Running applications
- ✓ Windows registry
- ✓ LSPs
- ADS
- Hosts file
- MRUs
- ✓ Browser hijacks
- ✓ Tracking cookies
- ✓ Rootkits
- Archives
- ✓ Executable files only
- ✓ Anti-Virus engine
- ✓ Spyware Heuristics

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-malware product prior to installing and using Ad-Aware, we recommend performing a Full Scan.

Full Scan

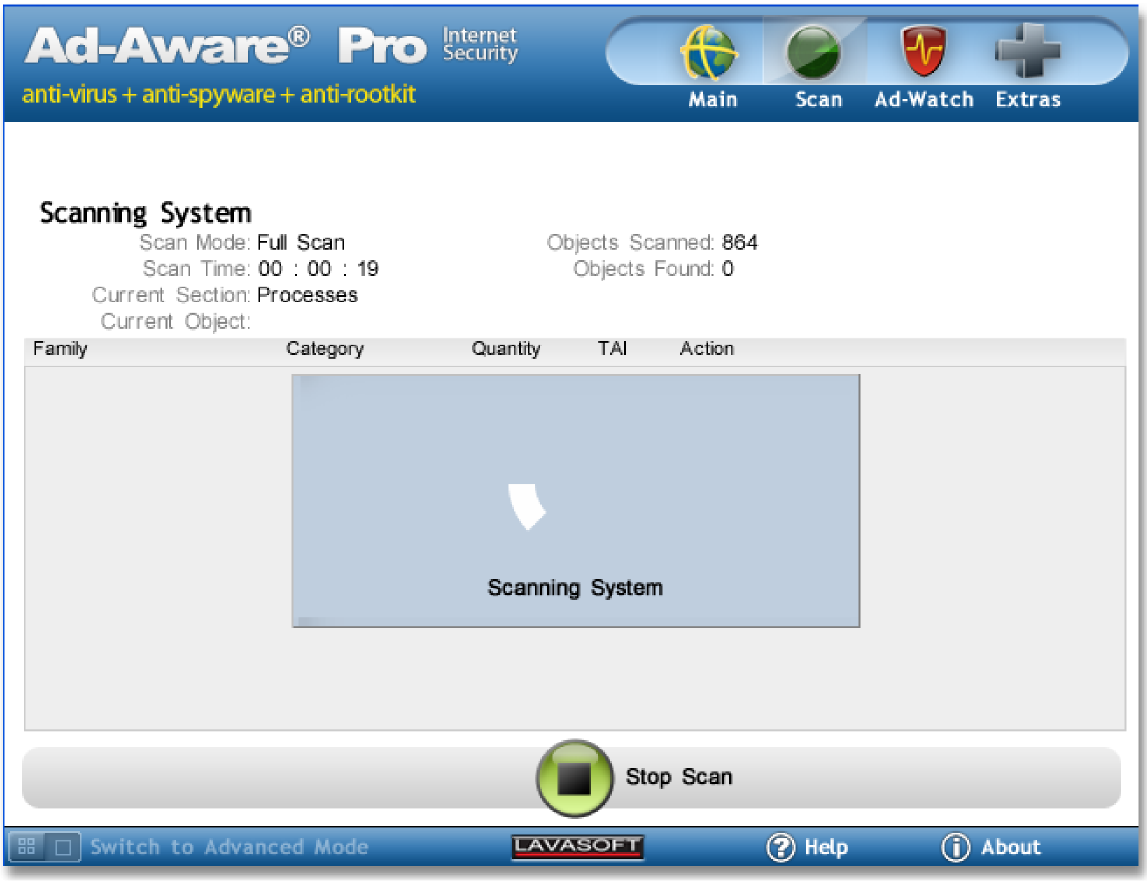
The "Full Scan" is an in-depth scan mode that thoroughly scans your entire system including all local drives. We recommend using the Full Scan when you use Ad-Aware for the first time, and at regular intervals to ensure that your system is clean. The Full Scan takes longer to scan your system than the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


Ad-Aware® Pro Internet Security
anti-virus + anti-spyware + anti-rootkit
Main
Scan
Ad-Watch
Extras
Stop Scan
Switch to Advanced Mode
LAVASOFT
Help
About

Scanning System

Scan Mode: Full Scan

Scan Time: 00 : 00 : 19

Current Section: Processes

Current Object:

Objects Scanned: 864

Objects Found: 0

Family	Category	Quantity	TAI	Action

Scanning System

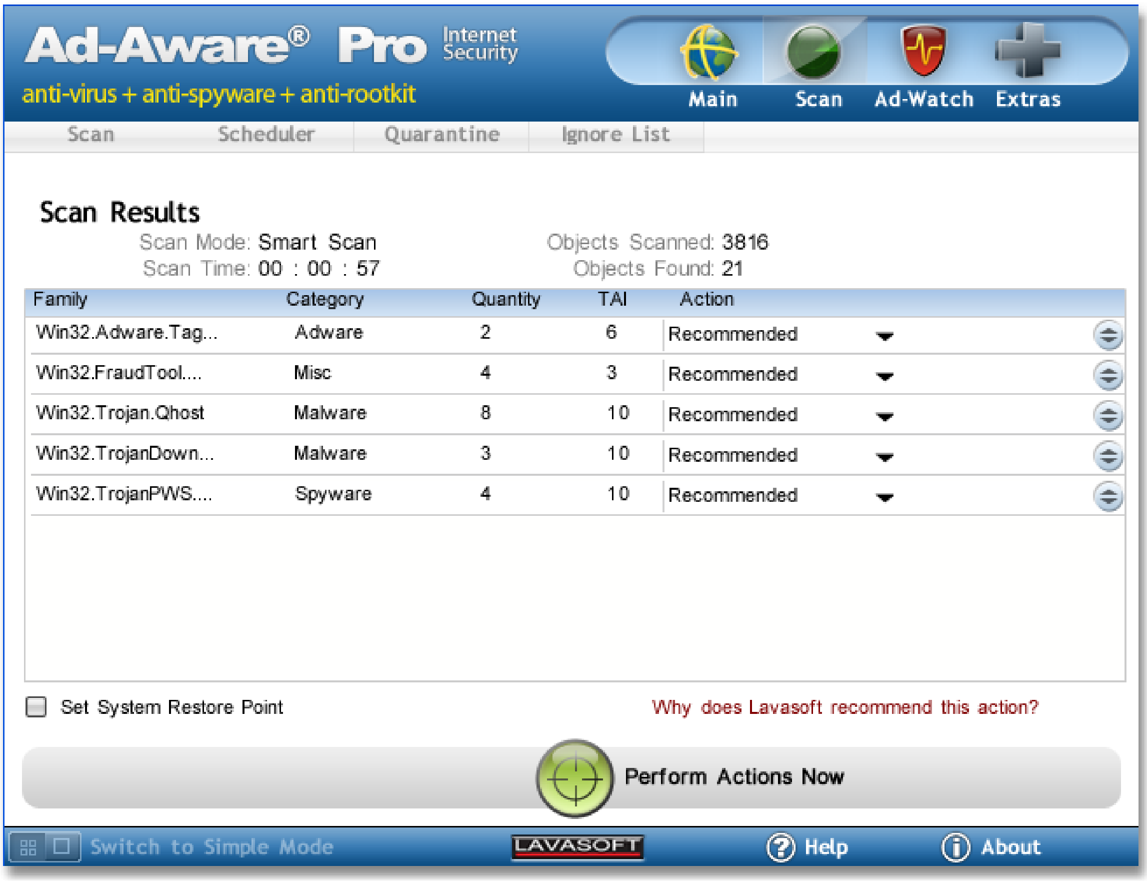
While Ad-Aware scans the system, the "Scanning System" menu displays the following:

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.



Scan Results

Scan Mode: Smart Scan
Scan Time: 00 : 00 : 57
Objects Scanned: 3816
Objects Found: 21

Family	Category	Quantity	TAI	Action
Win32.Adware.Tag...	Adware	2	6	Recommended
Win32.FraudTool....	Misc	4	3	Recommended
Win32.Trojan.Qhost	Malware	8	10	Recommended
Win32.TrojanDown...	Malware	3	10	Recommended
Win32.TrojanPWS....	Spyware	4	10	Recommended

□ Set System Restore Point

Why does Lavasoft recommend this action?

Perform Actions Now

In the “Scan Results” screen, detected objects are grouped by which family they belong to. The category 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.

Category

Provides more information about the behavior of the detected object.

Quantity

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.

- **Quarantine all:** Add all objects for a particular family to the Quarantine; isolate and back-up the object in quarantine, where it does not pose a threat to your system.
- **Remove all:** Delete all objects for a particular family from your system.
- **Repair all:** Ad-Aware will attempt to repair all objects for a particular family.
- **Allow all Once:** Allow the objects for a particular family to stay on the system. During the next scan, the objects will be detected again.
- **Add all To Ignore List:** Add the objects to the Ignore List; keep the items on your system and make sure it is not detected in future scans.

Note: Selected action for a particular family will be applied only to objects that selected action can be applied to.

To change an Action for single detected object from the recommended action, choose custom and select one of the following custom actions.

- **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.
- **Allow Once:** Allow the object to stay on the system. During the next scan, the object will be detected again.
- **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.
- **Repair:** Repair detected object (available only for specific objects).

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.

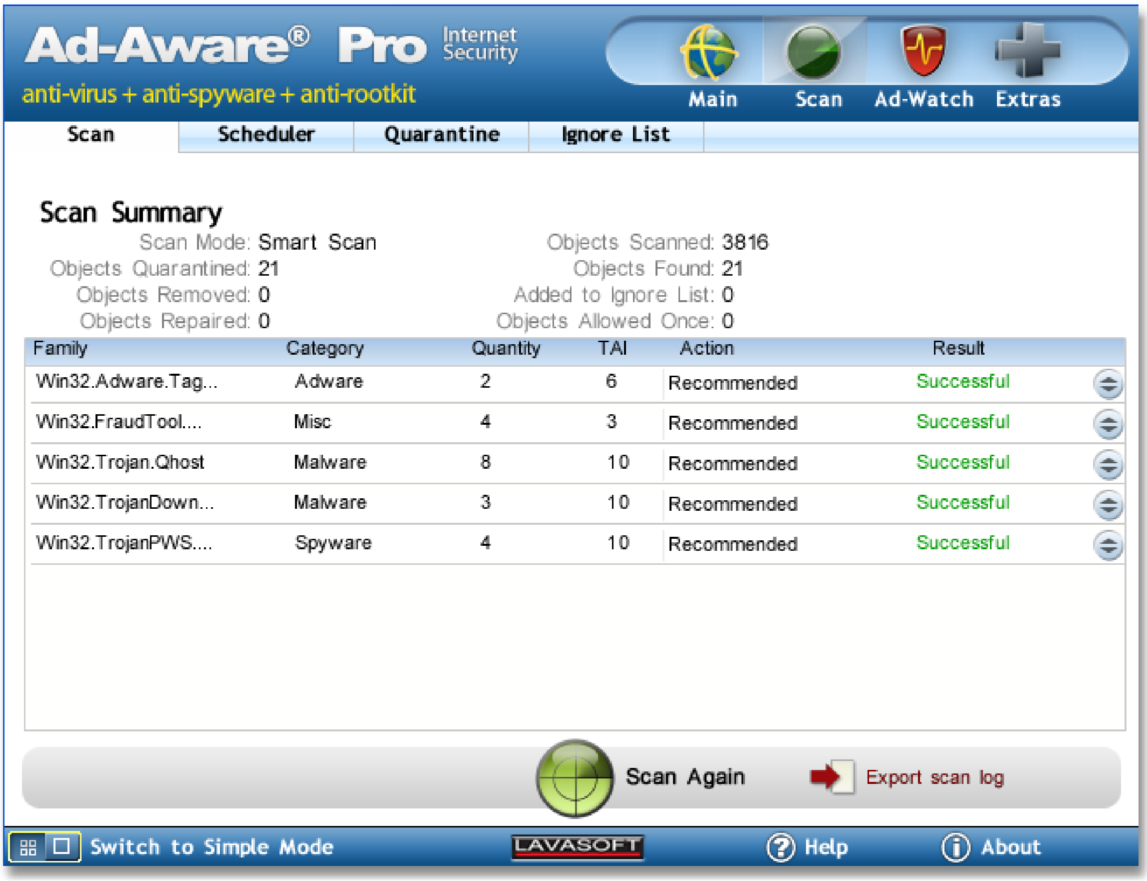
Select the required action for each object from the drop-down menu and then click "Perform Actions Now".
Ad-Aware will apply the required action for each detected object and present you with the "Scan Summary” screen.

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 Result is also shown.

Scan Result

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.



Scan Summary

Scan Mode: Smart Scan
Objects Quarantined: 21
Objects Removed: 0
Objects Repaired: 0
Objects Scanned: 3816
Objects Found: 21
Added to Ignore List: 0
Objects Allowed Once: 0

Family	Category	Quantity	TAI	Action	Result
Win32.Adware.Tag...	Adware	2	6	Recommended	Successful
Win32.FraudTool....	Misc	4	3	Recommended	Successful
Win32.Trojan.Qhost	Malware	8	10	Recommended	Successful
Win32.TrojanDown...	Malware	3	10	Recommended	Successful
Win32.TrojanPWS....	Spyware	4	10	Recommended	Successful

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

The following information is included in the Contents of the 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

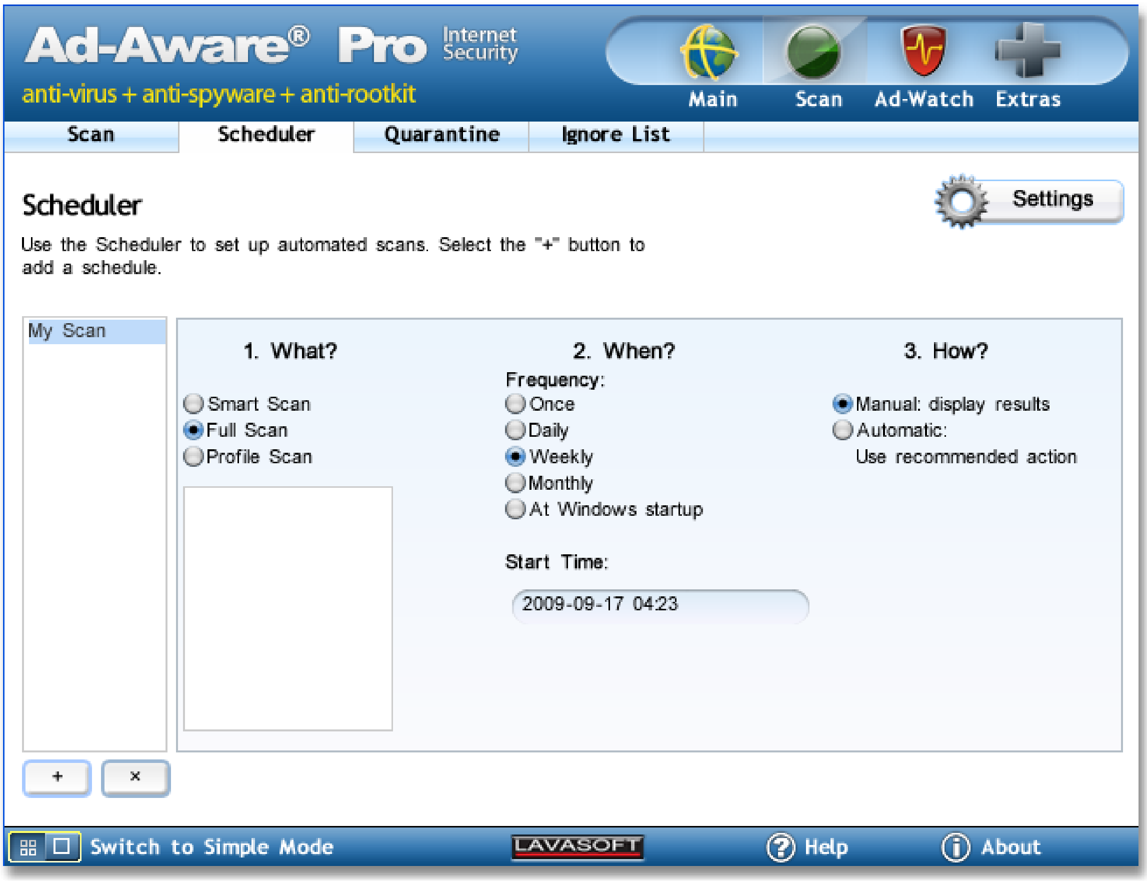
Settings:
List of Ad-Aware Scan Settings

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.



Scheduler

Use the Scheduler to set up automated scans. Select the "+" button to add a schedule.

1. What?

○ Smart Scan
● Full Scan
○ Profile Scan

2. When?

Frequency:
○ Once
○ Daily
● Weekly
○ Monthly
○ At Windows startup

Start Time:
2009-09-17 04:23

3. How?

● Manual: display results
○ Automatic:
Use recommended action

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, select it from the list and click "**x**".

Choose the scheduled scan settings.

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.

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, category, quantity 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.

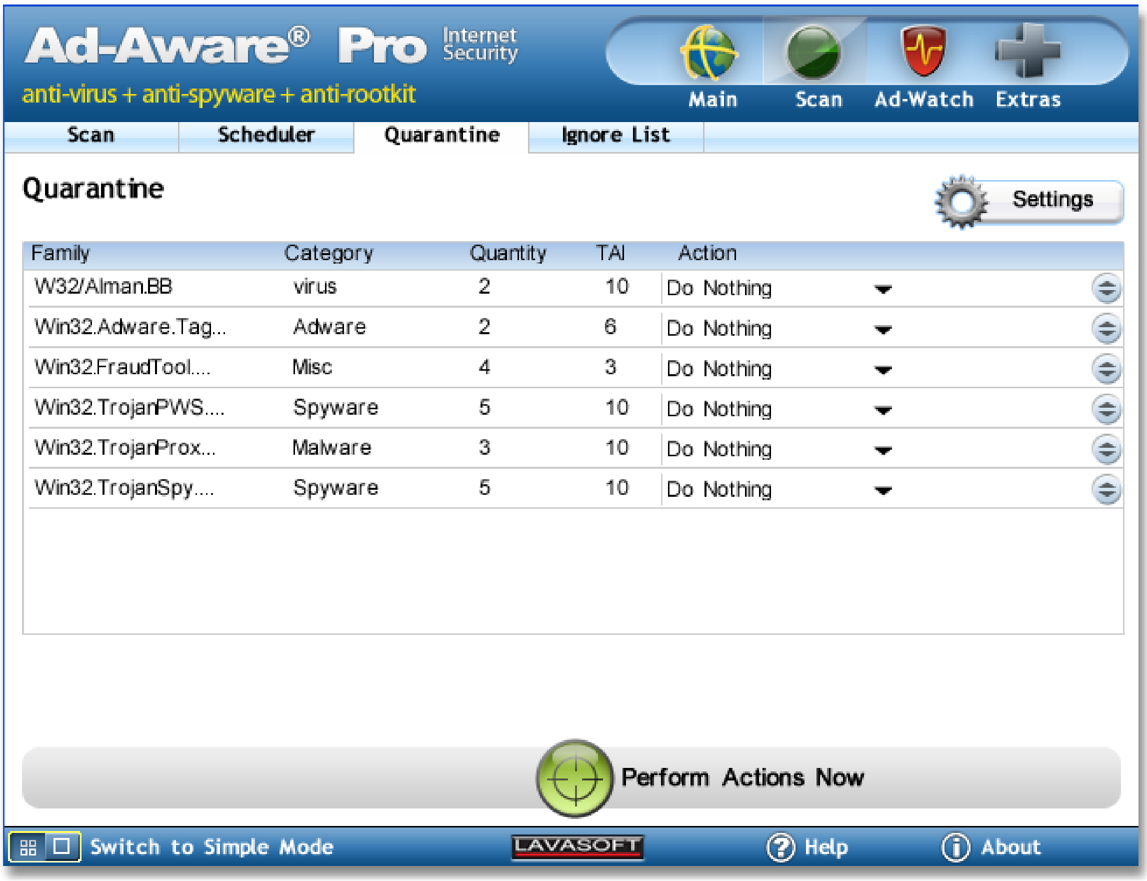
Remove Quarantined Objects

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.



Quarantine

Family	Category	Quantity	TAI	Action
W32/Alman.BB	virus	2	10	Do Nothing
Win32.Adware.Tag...	Adware	2	6	Do Nothing
Win32.FraudTool....	Misc	4	3	Do Nothing
Win32.TrojanPWS....	Spyware	5	10	Do Nothing
Win32.TrojanProx...	Malware	3	10	Do Nothing
Win32.TrojanSpy....	Spyware	5	10	Do Nothing

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.

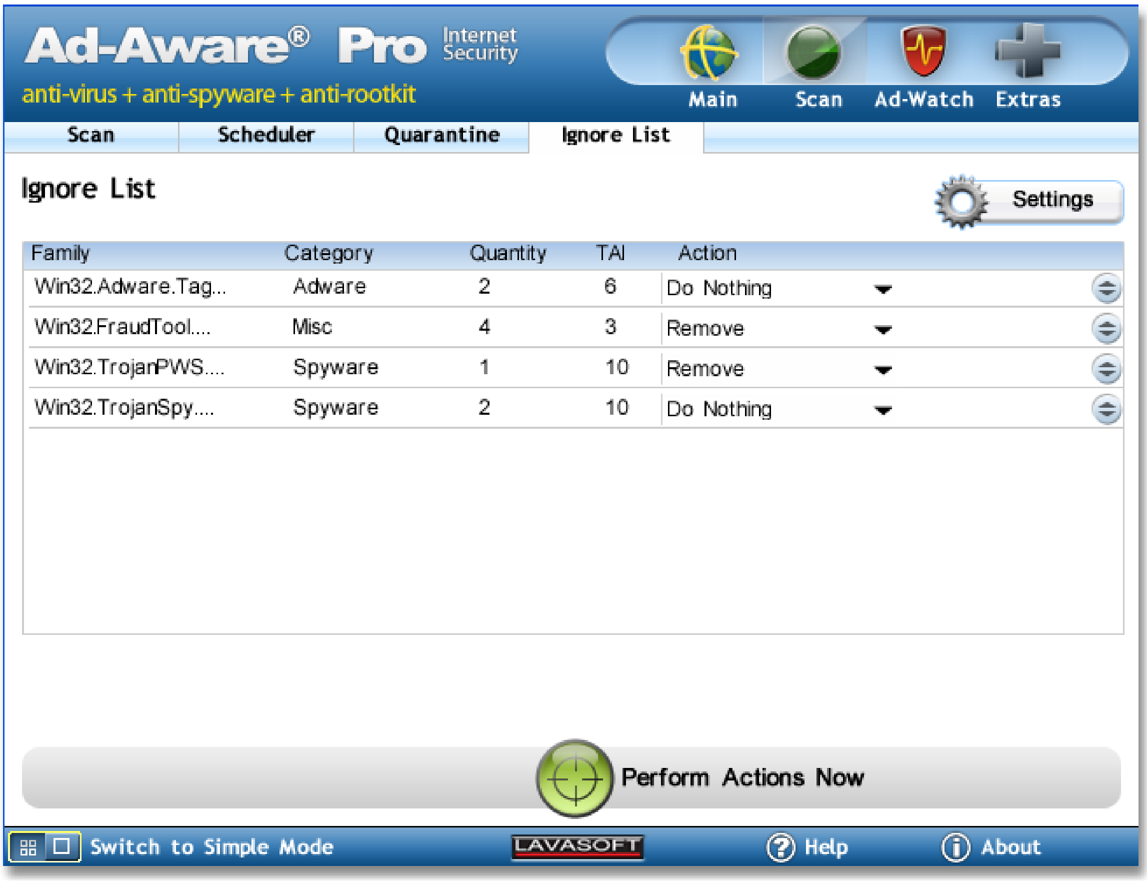
Remove Objects from Ignore List

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.

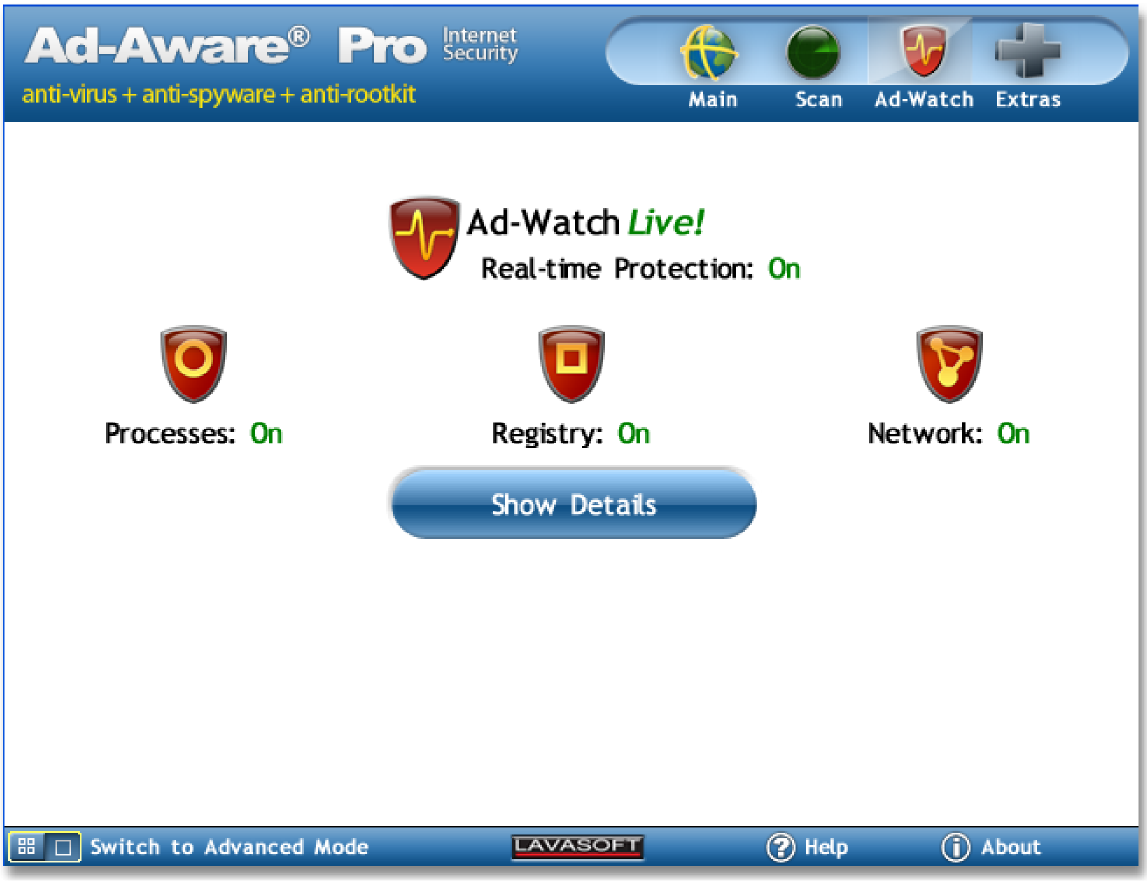


Ignore List

Family	Category	Quantity	TAI	Action
Win32.Adware.Tag...	Adware	2	6	Do Nothing
Win32.FraudTool....	Misc	4	3	Remove
Win32.TrojanPWS....	Spyware	1	10	Remove
Win32.TrojanSpy....	Spyware	2	10	Do Nothing

Ad-Watch

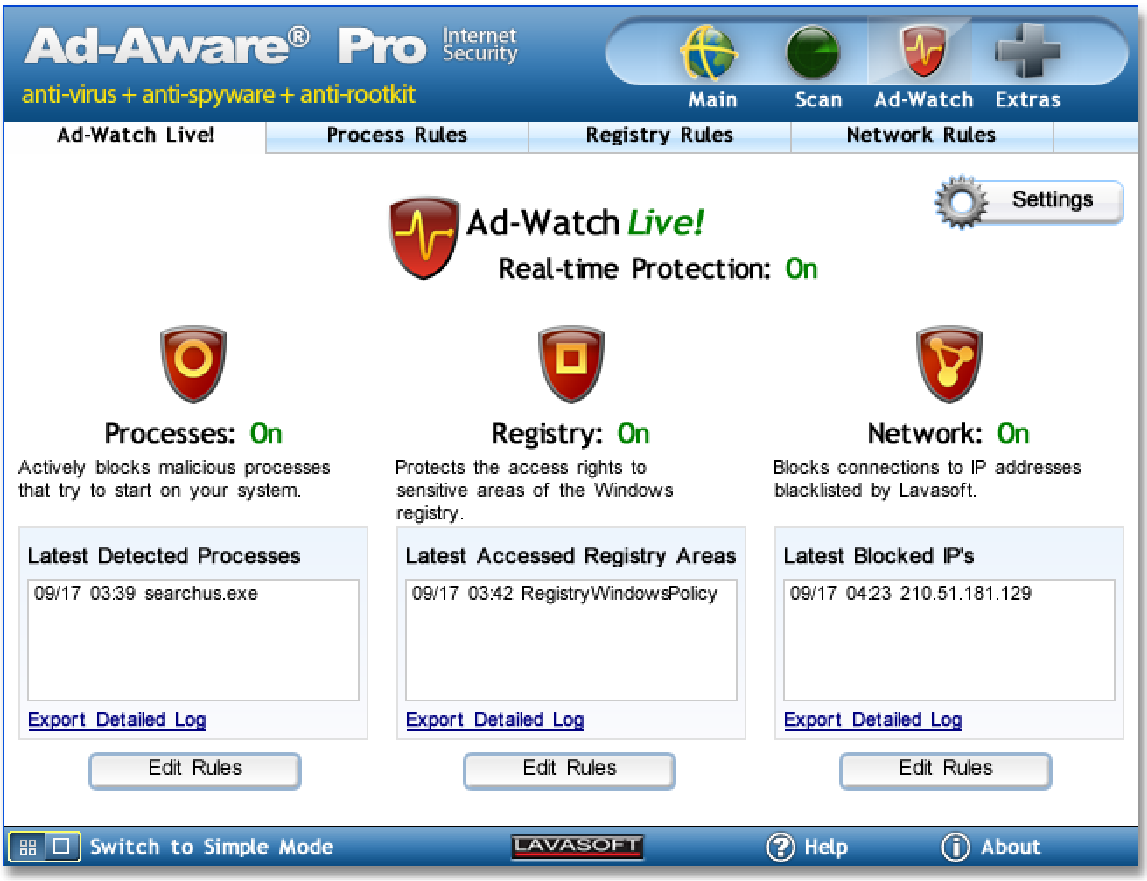
Click the “Ad-Watch” menu button to open the “Ad-Watch *Live*” screen.
Ad-Watch *Live!* is the real-time monitor featured in Ad-Aware. The scanner in Ad-Aware detects and cleans malware and viruses from your system, but Ad-Watch goes a step further. From the moment your machine is turned on, Ad-Watch *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 "Show Details" to show the latest detected processes, accessed registry areas and blocked IP addresses. To close the details window click "Hide Details".

Click to switch to Advanced Mode, to customize all the settings.

Ad-Watch Live



Ad-Watch *Live!*

Real-time Protection: On

Processes: On

Actively blocks malicious processes that try to start on your system.

Latest Detected Processes

09/17 03:39 searchus.exe

Export Detailed Log

Registry: On

Protects the access rights to sensitive areas of the Windows registry.

Latest Accessed Registry Areas

09/17 03:42 RegistryWindowsPolicy

Export Detailed Log

Network: On

Blocks connections to IP addresses blacklisted by Lavasoft.

Latest Blocked IP's

09/17 04:23 210.51.181.129

Export Detailed Log

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.(***Free***, ***Plus***, ***Pro***)
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***)

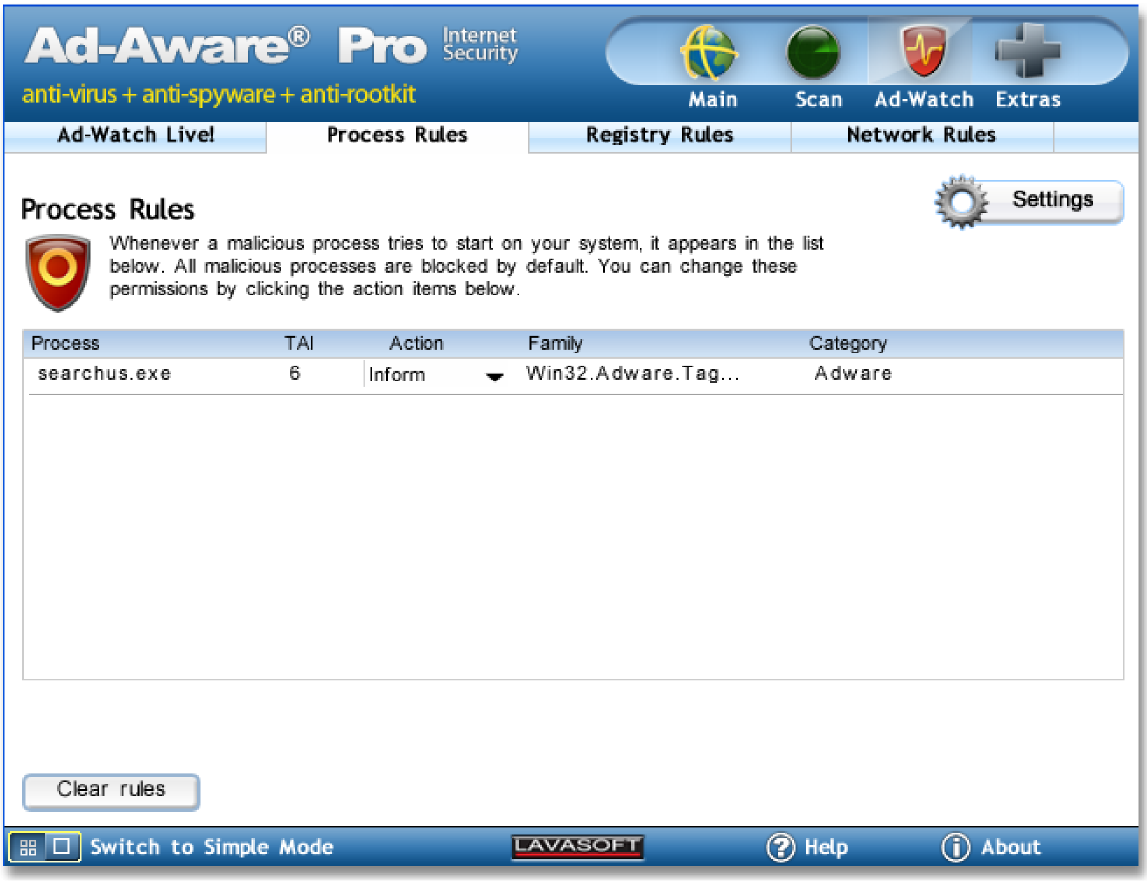
The Ad-Watch *Live!* real-time protection screen gives you a simple overview of the Ad-Watch *Live!* real-time monitor;
It shows if real-time protection is on or off, and allows you to turn each module on or off by simply clicking on the icon.
Note: If the icon is disabled, then the software has not 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 "Export Detailed Log" 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



Process Rules

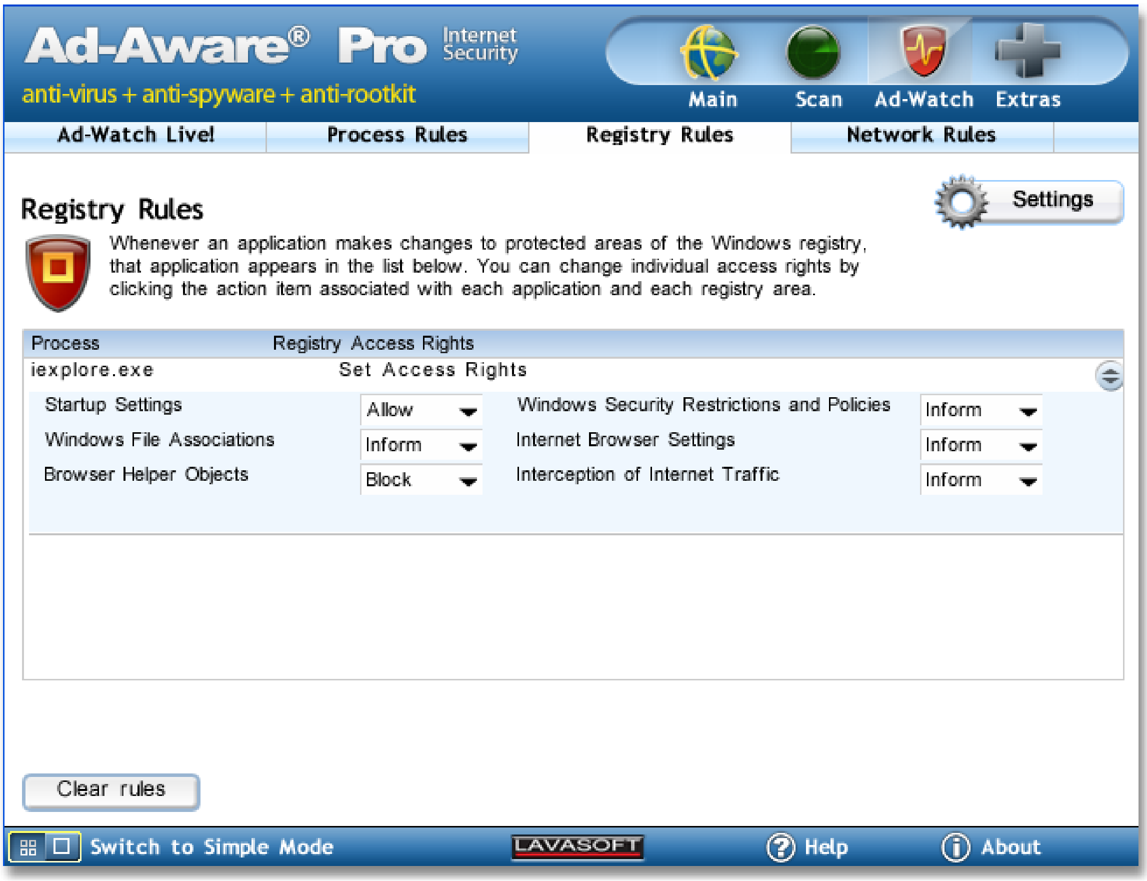
Whenever a malicious process tries to start on your system, it appears in the list below. All malicious processes are blocked by default. You can change these permissions by clicking the action items below.

Process	TAI	Action	Family	Category
searchus.exe	6	Inform	Win32.Adware.Tag...	Adware

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.

Registry Rules



Registry Rules

Whenever an application makes changes to protected areas of the Windows registry, that application appears in the list below. You can change individual access rights by clicking the action item associated with each application and each registry area.

Process	Registry Access Rights		
iexplore.exe	Set Access Rights		
Startup Settings	Allow	Windows Security Restrictions and Policies	Inform
Windows File Associations	Inform	Internet Browser Settings	Inform
Browser Helper Objects	Block	Interception of Internet Traffic	Inform

Every application that tries to change a registry area will be shown in this list.

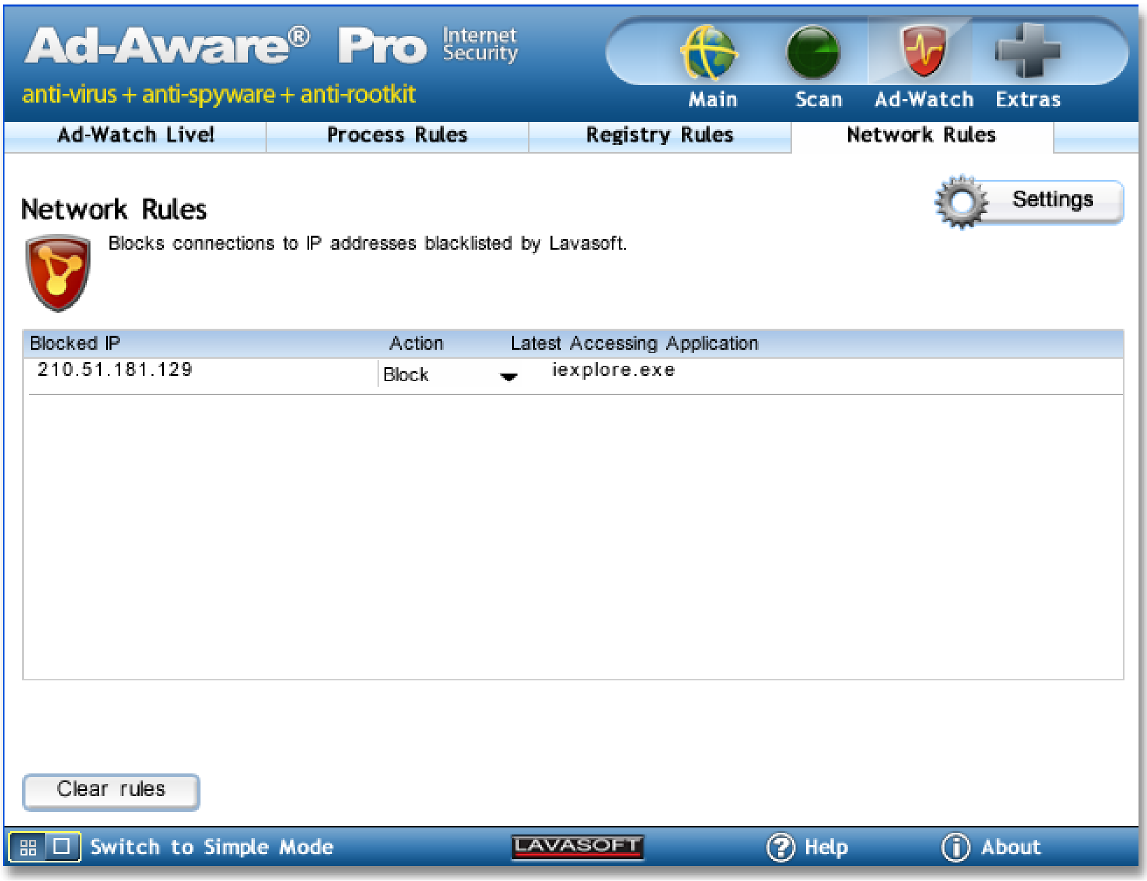
Ad-Watch *Live!* Registry protection allows you to protect the following areas of your registry:

- **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.

Network Rules



Network Rules

Blocks connections to IP addresses blacklisted by Lavasoft.

Blocked IP	Action	Latest Accessing Application
210.51.181.129	Block	iexplore.exe

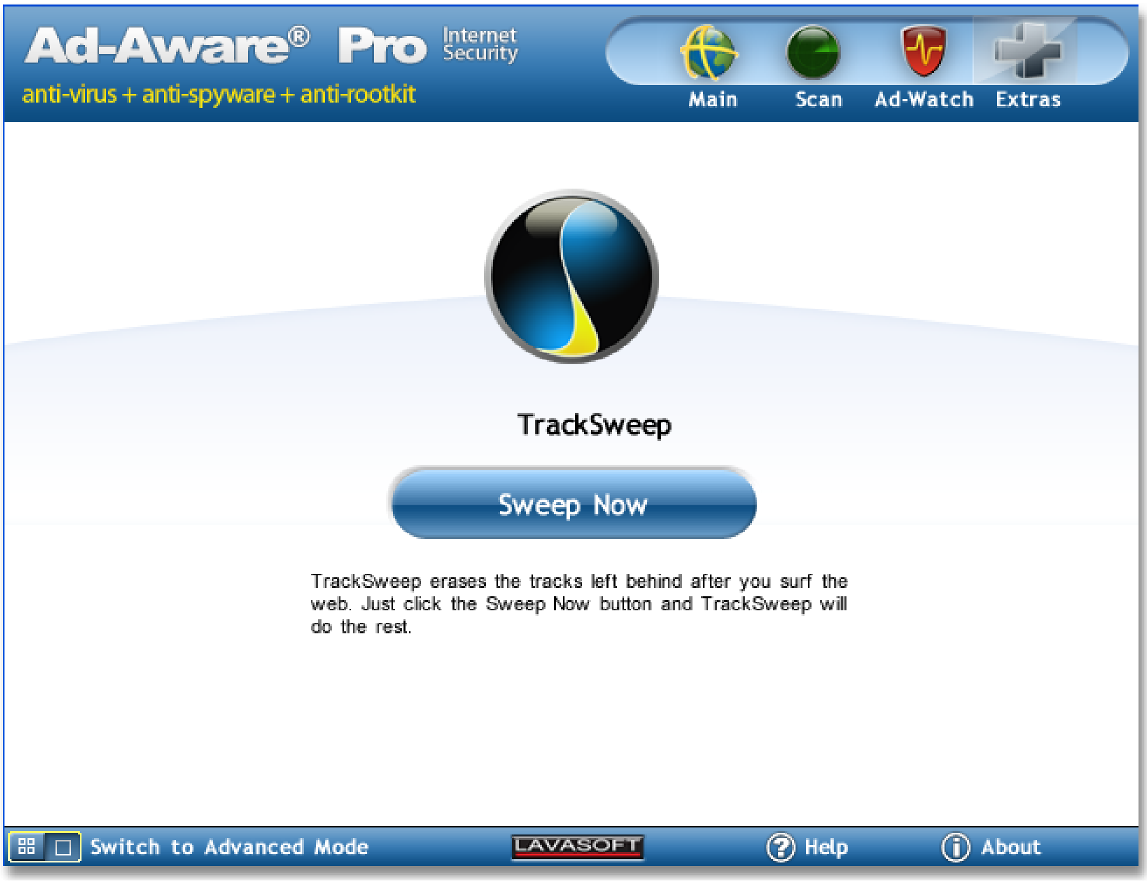
Real-time Network protection is designed to detect connections to blacklisted IP addresses. When any application connects to a blacklisted IP address that is detected as malicious, the Ad-Watch notification will inform you that it was blocked.

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.

Extras

Click the “Extras” menu button to open the extra "TrackSweep" feature.
Ad-Aware’s TrackSweep feature is a privacy tool that allows you to remove all traces of your Internet browsing from your system.



TrackSweep erases the tracks left behind after you surf the web. Just click the Sweep Now button and TrackSweep will do the rest.

Click "Sweep Now" to remove all traces of your Internet browsing from your system.
Please ensure that the internet browser is closed, if the internet browser is open Ad-Aware will request you to close it, so that TrackSweep can run.

Click to switch to Advanced Mode, to customize all the settings.

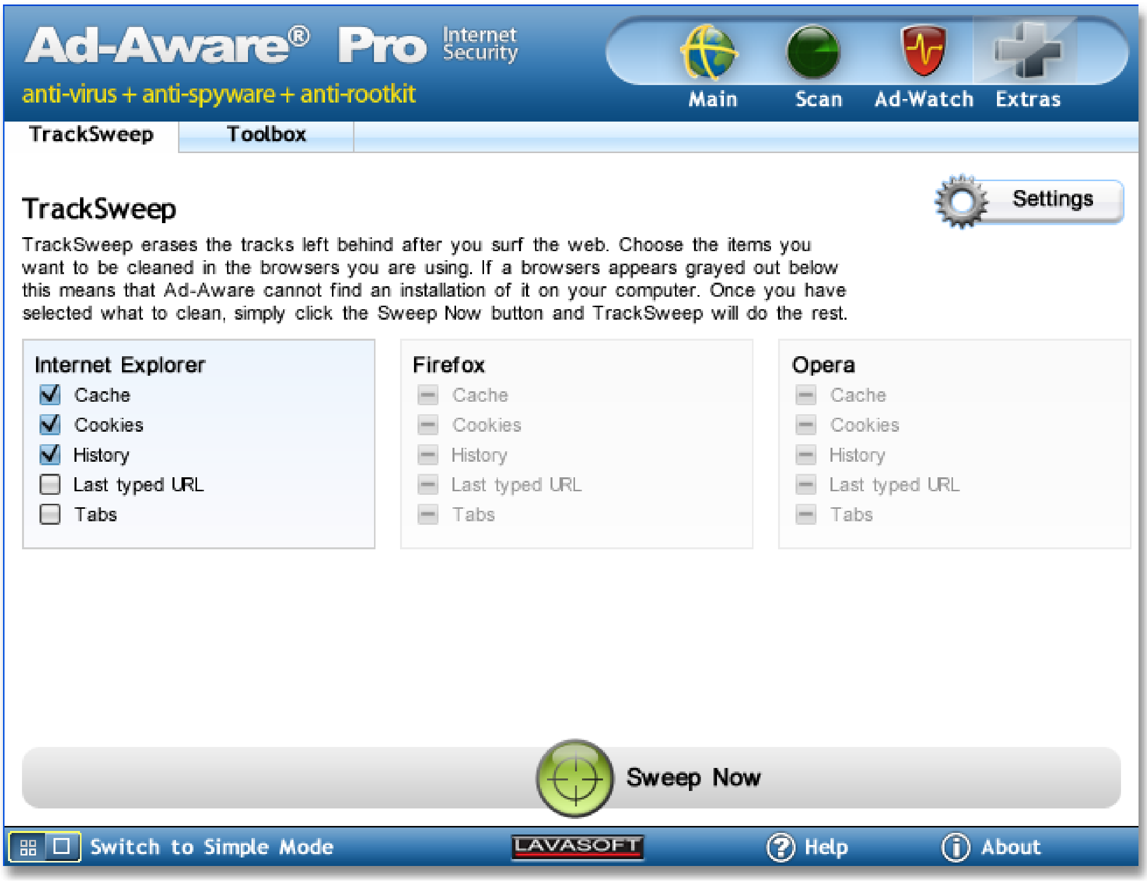
TrackSweep

Click the “Extras” menu button to open the extra "TrackSweep" feature.
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. Web browsers that are not installed on your computer will be grayed out.

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



TrackSweep

TrackSweep erases the tracks left behind after you surf the web. Choose the items you want to be cleaned in the browsers you are using. If a browsers appears grayed out below this means that Ad-Aware cannot find an installation of it on your computer. Once you have selected what to clean, simply click the Sweep Now button and TrackSweep will do the rest.

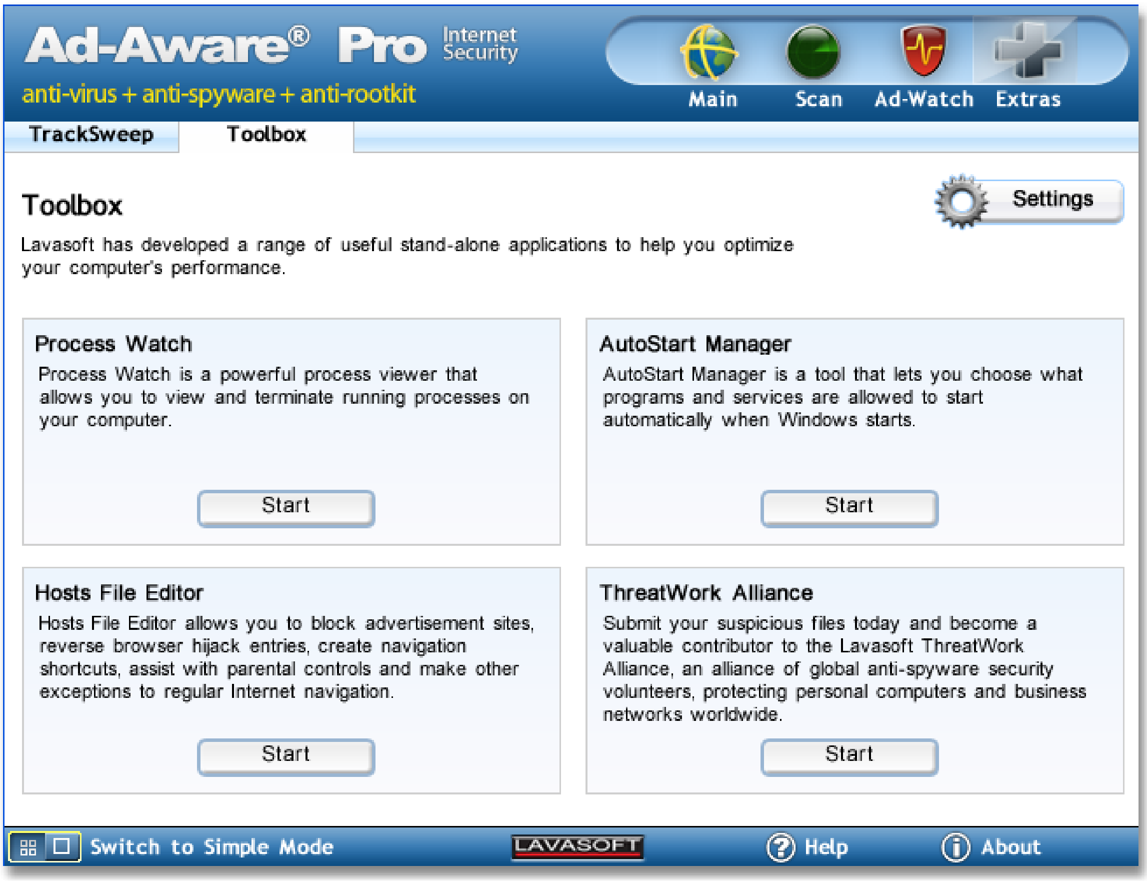
Internet Explorer
☑ Cache
☑ Cookies
☑ History
□ Last typed URL
□ Tabs

Firefox
⊟ Cache
⊟ Cookies
⊟ History
⊟ Last typed URL
⊟ Tabs

Opera
⊟ Cache
⊟ Cookies
⊟ History
⊟ Last typed URL
⊟ Tabs

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.



Toolbox

Lavasoft has developed a range of useful stand-alone applications to help you optimize your computer's performance.

Process Watch

Process Watch is a powerful process viewer that allows you to view and terminate running processes on your computer.

AutoStart Manager

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

Hosts File Editor

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.

ThreatWork Alliance

Submit your suspicious files today and become a valuable contributor to the Lavasoft ThreatWork Alliance, an alliance of global anti-spyware security volunteers, protecting personal computers and business networks worldwide.

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.

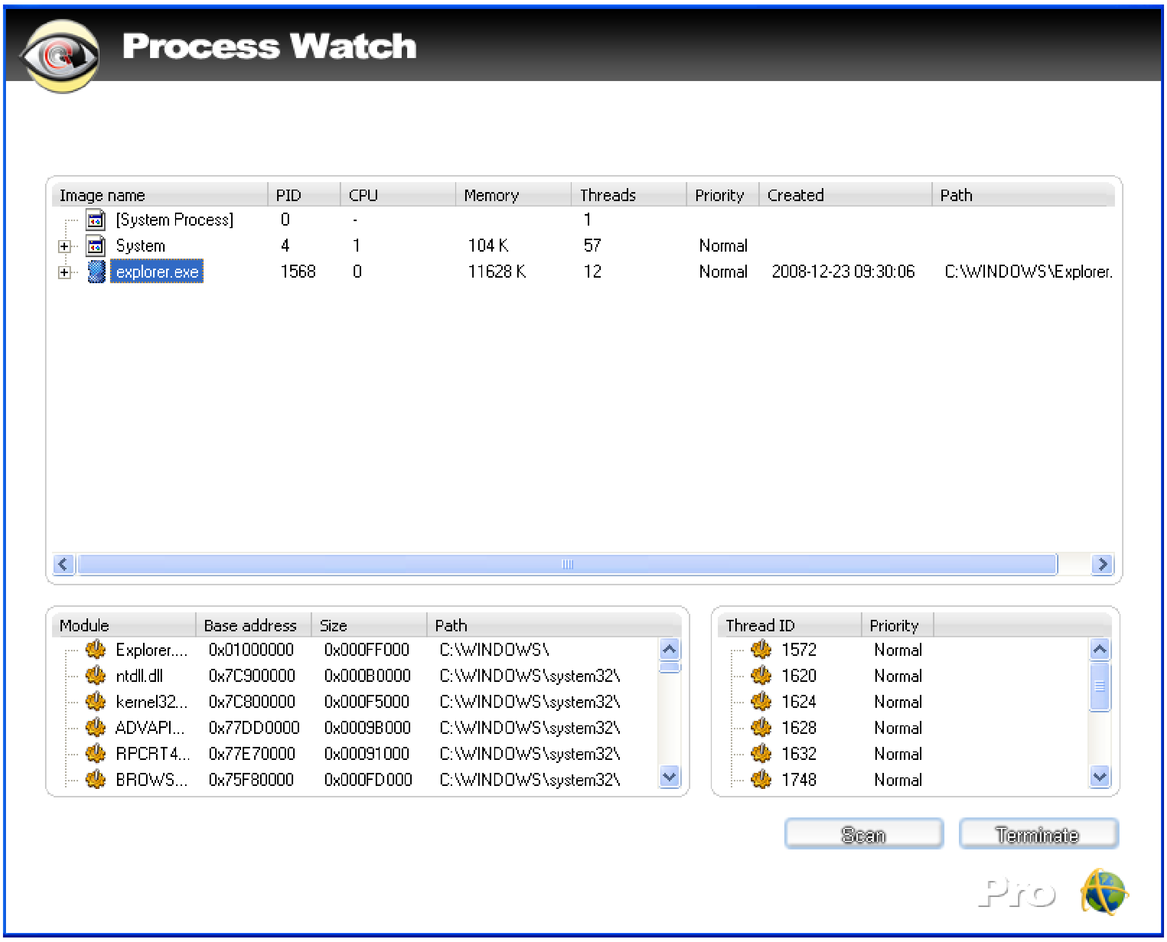


Image name	PID	CPU	Memory	Threads	Priority	Created	Path
[System Process]	0	-		1			
System	4	1	104 K	57	Normal		
explorer.exe	1568	0	11628 K	12	Normal	2008-12-23 09:30:06	C:\WINDOWS\Explorer.

Module	Base address	Size	Path
Explorer....	0x01000000	0x000FF000	C:\WINDOWS\
ntdll.dll	0x7C900000	0x000B0000	C:\WINDOWS\system32\
kernel32...	0x7C800000	0x000F5000	C:\WINDOWS\system32\
ADVAPI...	0x77DD0000	0x0009B000	C:\WINDOWS\system32\
RPCRT4...	0x77E70000	0x00091000	C:\WINDOWS\system32\
BROWS...	0x75F80000	0x000FD000	C:\WINDOWS\system32\

Thread ID	Priority
1572	Normal
1620	Normal
1624	Normal
1628	Normal
1632	Normal
1748	Normal

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.

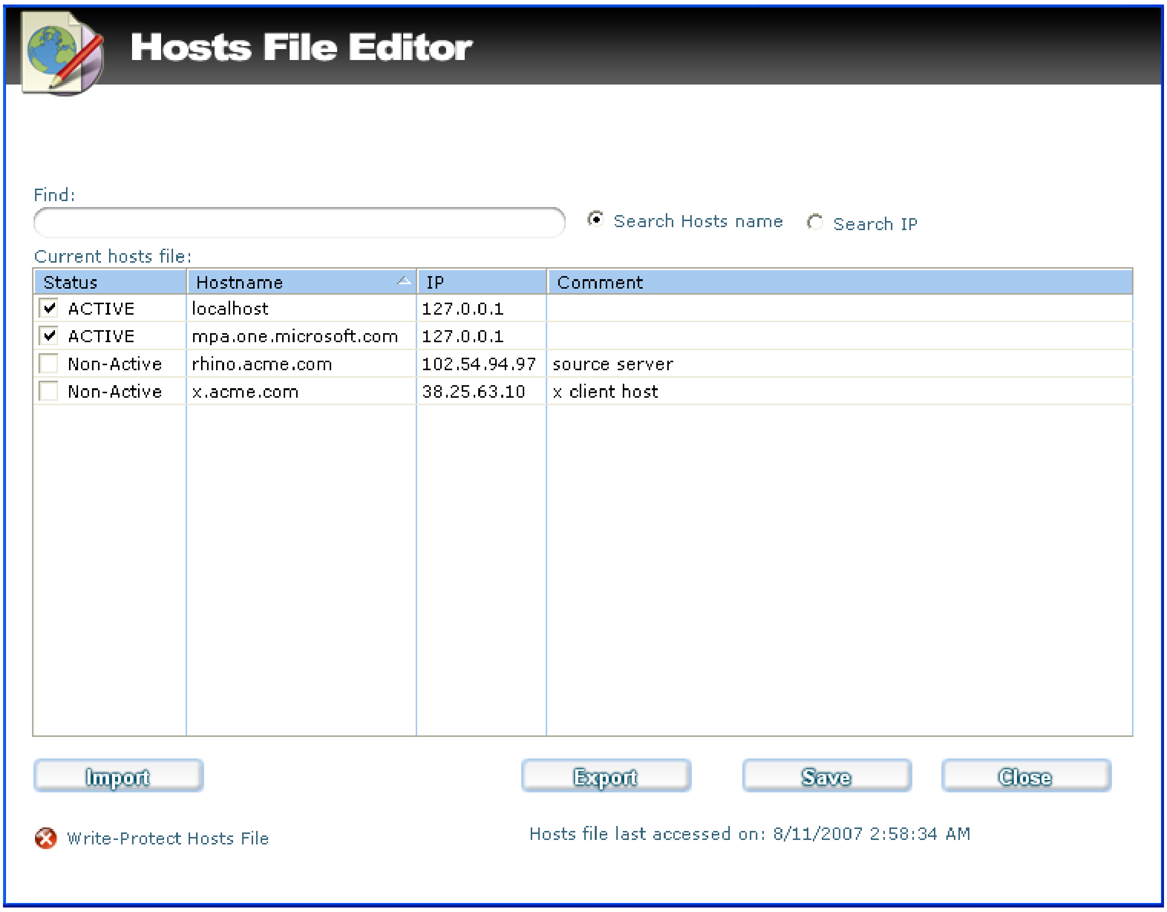
The thread window lists information by:

- **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.



Find:

● Search Hosts name ○ Search IP

Current hosts file:

Status	Hostname	IP	Comment
☑ ACTIVE	localhost	127.0.0.1	
☑ ACTIVE	mpa.one.microsoft.com	127.0.0.1	
□ Non-Active	rhino.acme.com	102.54.94.97	source server
□ Non-Active	x.acme.com	38.25.63.10	x client host

Hosts file last accessed on: 8/11/2007 2:58:34 AM

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.

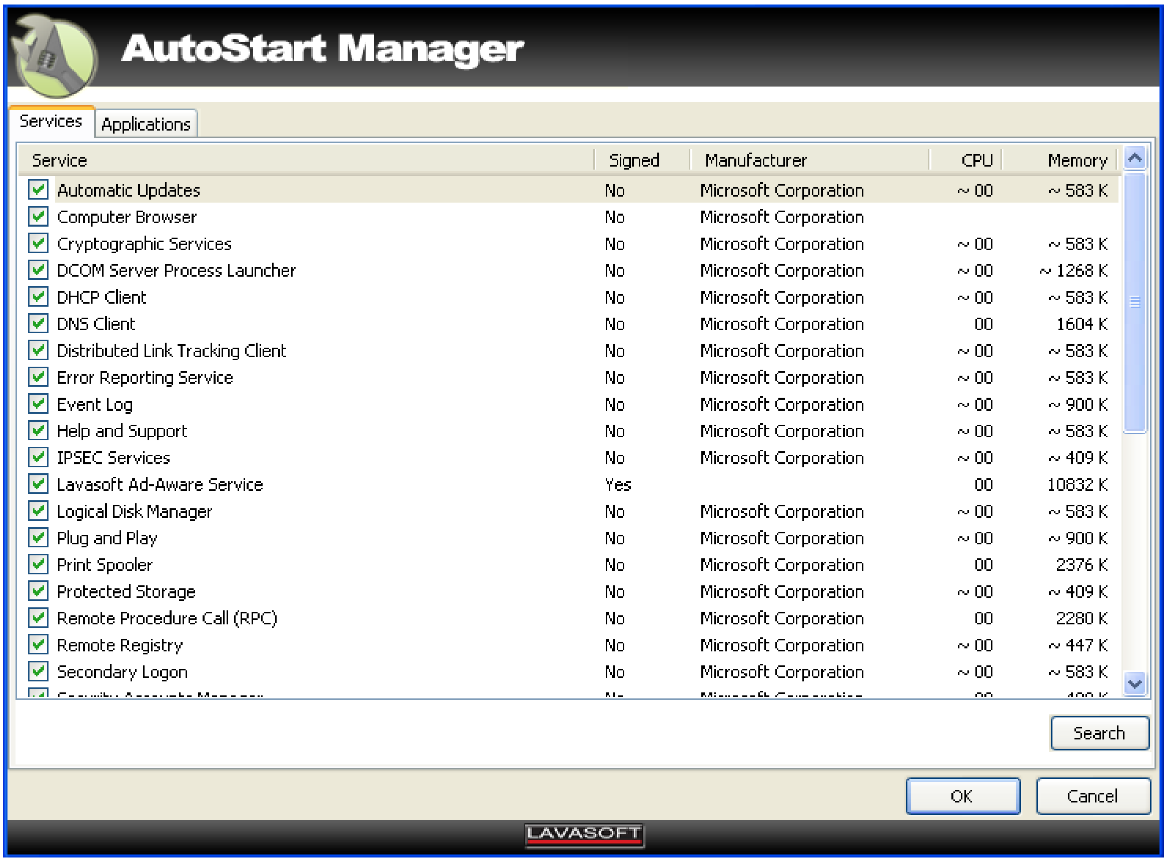
Click "Save" to save the changes you made.

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.



Service	Signed	Manufacturer	CPU	Memory
☑ Automatic Updates	No	Microsoft Corporation	~ 00	~ 583 K
☑ Computer Browser	No	Microsoft Corporation		
☑ Cryptographic Services	No	Microsoft Corporation	~ 00	~ 583 K
☑ DCOM Server Process Launcher	No	Microsoft Corporation	~ 00	~ 1268 K
☑ DHCP Client	No	Microsoft Corporation	~ 00	~ 583 K
☑ DNS Client	No	Microsoft Corporation	00	1604 K
☑ Distributed Link Tracking Client	No	Microsoft Corporation	~ 00	~ 583 K
☑ Error Reporting Service	No	Microsoft Corporation	~ 00	~ 583 K
☑ Event Log	No	Microsoft Corporation	~ 00	~ 900 K
☑ Help and Support	No	Microsoft Corporation	~ 00	~ 583 K
☑ IPSEC Services	No	Microsoft Corporation	~ 00	~ 409 K
☑ Lavasoft Ad-Aware Service	Yes		00	10832 K
☑ Logical Disk Manager	No	Microsoft Corporation	~ 00	~ 583 K
☑ Plug and Play	No	Microsoft Corporation	~ 00	~ 900 K
☑ Print Spooler	No	Microsoft Corporation	00	2376 K
☑ Protected Storage	No	Microsoft Corporation	~ 00	~ 409 K
☑ Remote Procedure Call (RPC)	No	Microsoft Corporation	00	2280 K
☑ Remote Registry	No	Microsoft Corporation	~ 00	~ 447 K
☑ Secondary Logon	No	Microsoft Corporation	~ 00	~ 583 K

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.

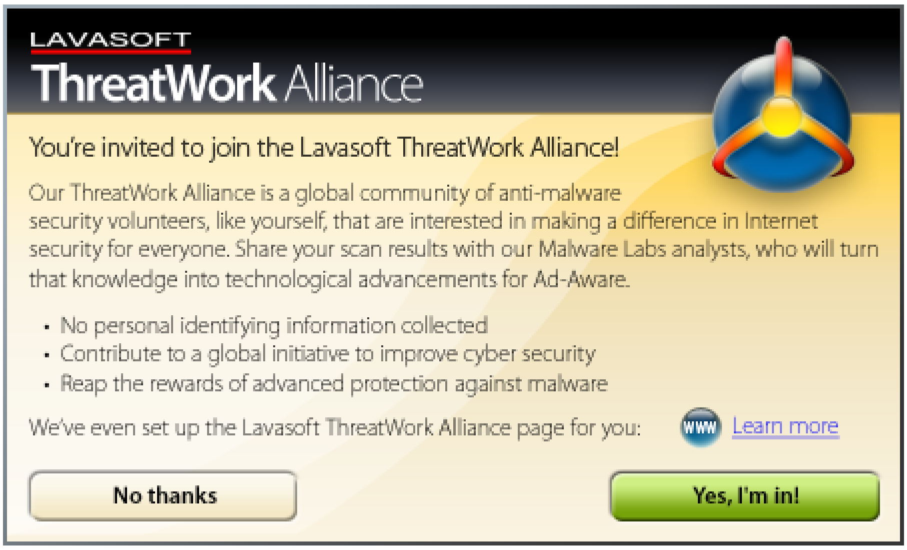
You can choose from the following operations:

- **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.

Lavasoft ThreatWork Alliance

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

The first time you open Ad-Aware after installation, you will be presented with the following invitation to join Lavasoft Threatwork.
Click "Yes, I'm in!" to join or "No thanks" to close this window.



LAVASOFT
ThreatWork Alliance

You're invited to join the Lavasoft ThreatWork Alliance!

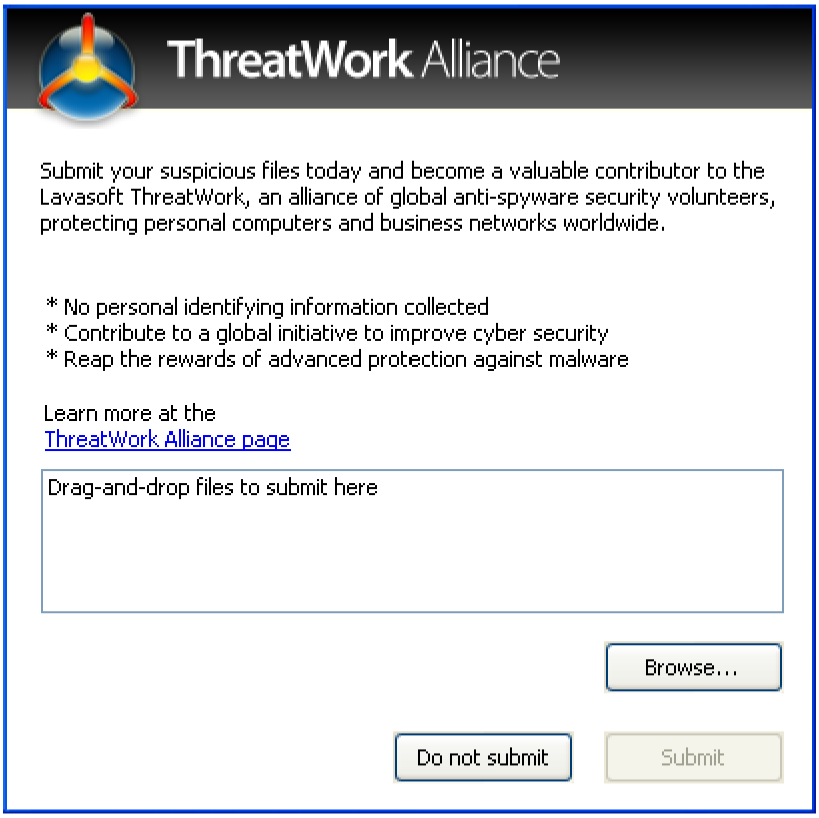
Our ThreatWork Alliance is a global community of anti-malware security volunteers, like yourself, that are interested in making a difference in Internet security for everyone. Share your scan results with our Malware Labs analysts, who will turn that knowledge into technological advancements for Ad-Aware.

- No personal identifying information collected
- Contribute to a global initiative to improve cyber security
- Reap the rewards of advanced protection against malware

We've even set up the Lavasoft ThreatWork Alliance page for you:

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

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



Submit your suspicious files today and become a valuable contributor to the Lavasoft ThreatWork, an alliance of global anti-spyware security volunteers, protecting personal computers and business networks worldwide.

* No personal identifying information collected
* Contribute to a global initiative to improve cyber security
* Reap the rewards of advanced protection against malware

Learn more at the
ThreatWork Alliance page

Drag-and-drop files to submit here

More information about the Lavasoft Threatwork Alliance can be found on our website by clicking here.

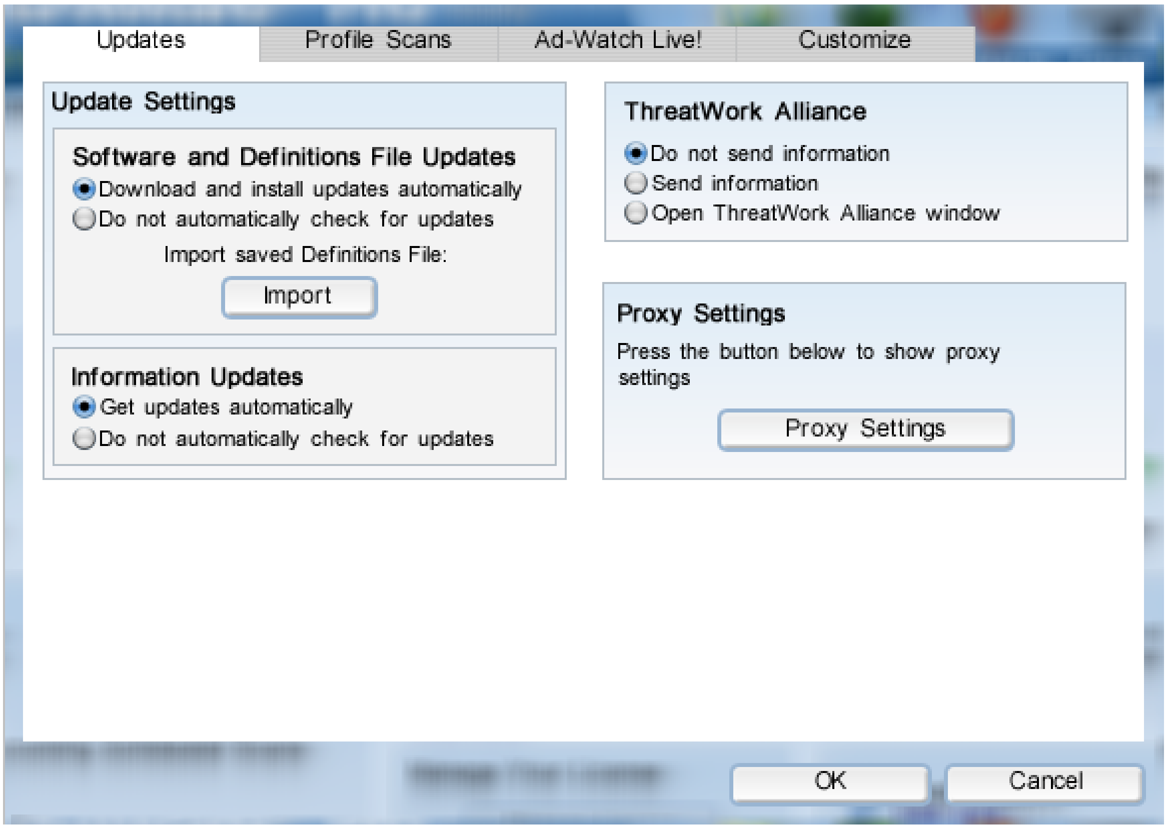
You can configure the Lavasoft ThreatWork Alliance settings in the Update tab of Ad-Aware's update settings.

Settings

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.

Updates

Configure the updates settings for the software and Definitions File, the ThreatWork Alliance, information and proxy settings.



Update Settings

Software and Definitions File Updates

● Download and install updates automatically

○ Do not automatically check for updates

Import saved Definitions File:

Information Updates

● Get updates automatically

○ Do not automatically check for updates

ThreatWork Alliance

● Do not send information

○ Send information

○ Open ThreatWork Alliance window

Proxy Settings

Press the button below to show 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

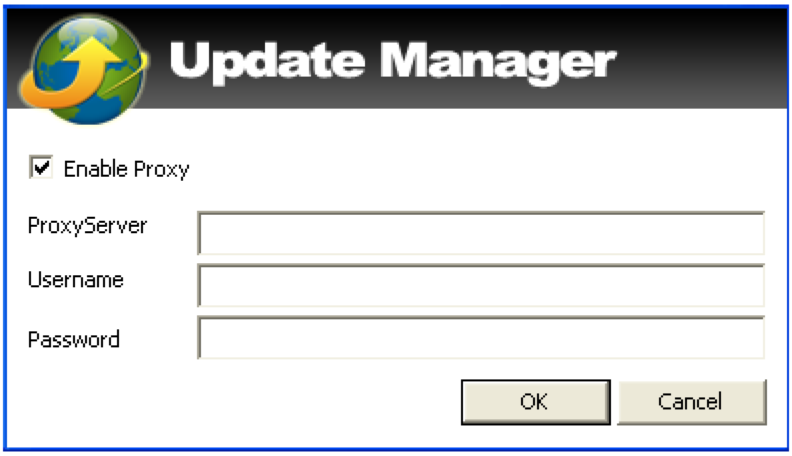
You can adjust the information updates to keep informed and updated about Lavasoft (company information, industry news, etc.) This is automatically displayed in the main status window.

ThreatWork Alliance Settings

You can configure the Lavasoft ThreatWork Alliance settings to automatically submit suspicious files silently (meaning you do not see the ThreatWork Alliance window), or to open the ThreatWork Alliance 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 the Lavasoft ThreatWork Alliance.

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.



Update Manager

☑ Enable Proxy

ProxyServer

Username

Password

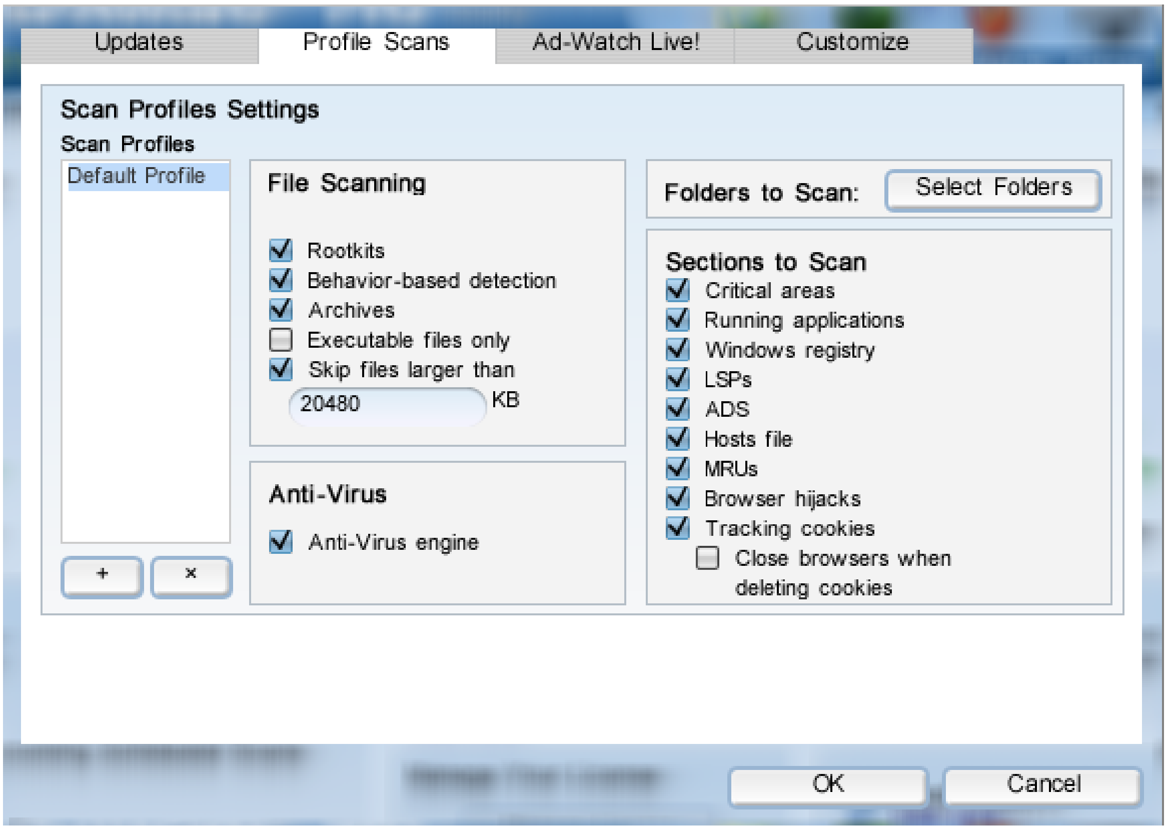
To Enable, tick the box beside "Enable Proxy", enter your proxy server address (in the format, proxyaddress:portnumber), your username and password and click 'Ok'.
To Disable, untick the "Enable Proxy" box and click "Ok".

Click "Ok" to apply any changes made.

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

Profile Scans

Configure the profile scanning settings.



Scan Profiles Settings

Scan Profiles

Default Profile

File Scanning

☑ Rootkits
☑ Behavior-based detection
☑ Archives
□ Executable files only
☑ Skip files larger than
20480 KB

Anti-Virus

☑ Anti-Virus engine

Folders to Scan:

Sections to Scan

☑ Critical areas
☑ Running applications
☑ Windows registry
☑ LSPs
☑ ADS
☑ Hosts file
☑ MRUs
☑ Browser hijacks
☑ Tracking cookies
□ Close browsers when deleting cookies

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.
Behavior-based detection: 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

Critical areas: Scans the critical areas of your computer.
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

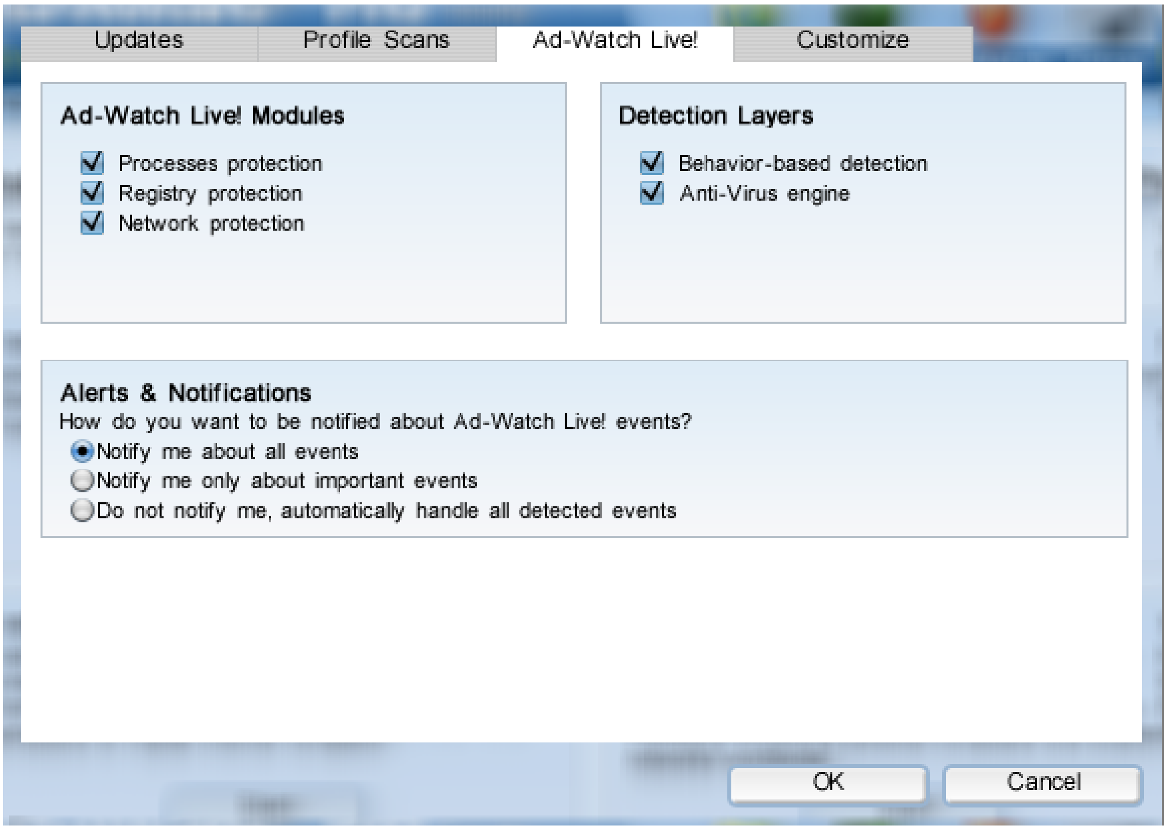
Anti-virus engine: Check this box to use Ad-Aware's extended anti-virus scanner.

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.



Ad-Watch Live! Modules

☑ Processes protection
☑ Registry protection
☑ Network protection

Detection Layers

☑ Behavior-based detection
☑ Anti-Virus engine

Alerts & Notifications

How do you want to be notified about Ad-Watch Live! events?

● Notify me about all events
○ Notify me only about important events
○ Do not notify me, automatically handle all detected events

Ad-Watch Live! Modules

Choose which Ad-Watch *Live!* modules to have on or off by clicking the box beside each module.

Detection Layers

Behavior-based detection: 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.

Alerts & Notifications

Choose how you want to be notified about Ad-Watch *Live!* events.

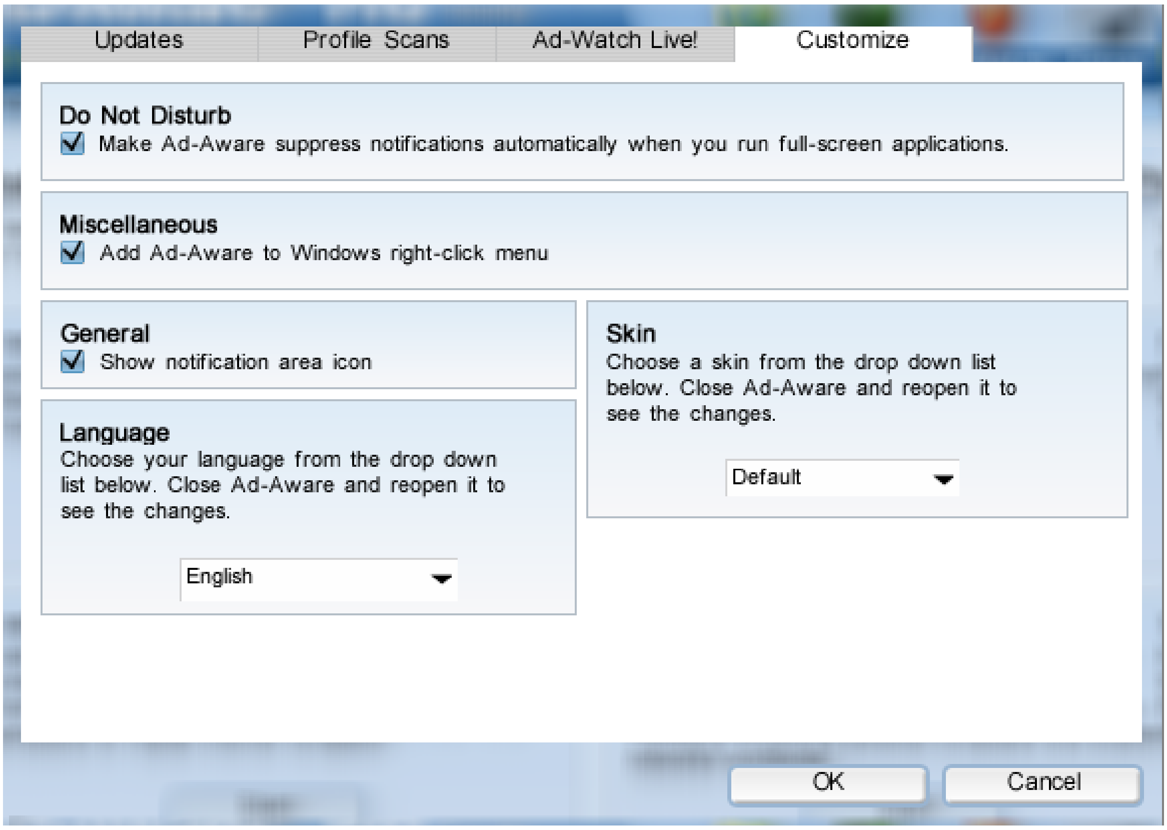
Notify me about all events: All information messages are displayed in the tray icon.
Notify me only about important events: Only important information messages are displayed in the tray icon.
Do not notify me, automatically handle all detected events: Events are automatically handled and no Ad-Watch 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.

Customize

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



Do Not Disturb
☑ Make Ad-Aware suppress notifications automatically when you run full-screen applications.

Miscellaneous
☑ Add Ad-Aware to Windows right-click menu

General
☑ Show notification area icon

Language
Choose your language from the drop down list below. Close Ad-Aware and reopen it to see the changes.
English

Skin
Choose a skin from the drop down list below. Close Ad-Aware and reopen it to see the changes.
Default

Do Not Disturb (*Pro*)

Do Not Disturb Mode is a non-intrusive, resource efficient mode designed to be used whenever you are using entertainment applications (e.g. games, movies) and do not want to be disturbed by notifications. Choose this option to suppress notifications automatically. Scheduled scans and scheduled updates will be suspended.

An Ad-Aware notification window (Events During Do Not Disturb Mode) will appear if events are detected while in Do Not Disturb Mode.

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.

General

Show notification area 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.

Since Ad-Aware is used my millions of people around the world, we get many requests for various translations of the user interface - from all corners of the globe. At Lavasoft, we are committed to making sure that computer users, regardless of their geographic location, have the power to protect their online privacy, so we have set up a community-based translations program where you can find Ad-Aware translations for languages that are not provided by Lavasoft in the official installation package. These translations have been developed by our global community of security volunteers, and are in turn shared with you to improve your Ad-Aware experience.

If you'd like to be a part of this community, sign-up to the MyLavasoft community at www.lavasoft.com, visit the Community Translations Project page, and join in the fun!

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.

In a similar spirit to the Community Translations Project, we are giving you the power to control the look of Ad-Aware by designing your own customized skin file, creating a new look and feel for Ad-Aware’s user interface. To create a skin file, sign-up to the MyLavasoft community at www.lavasoft.com, go to the Skin Creation Guide page, and join in the fun!

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 the Lavasoft ThreatWork Alliance.

Enter Do Not Disturb Mode/Exit Do Not Disturb Mode

Enters/Exits Do Not Disturb Mode.

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.

Update

Downloads and installs any available updates.

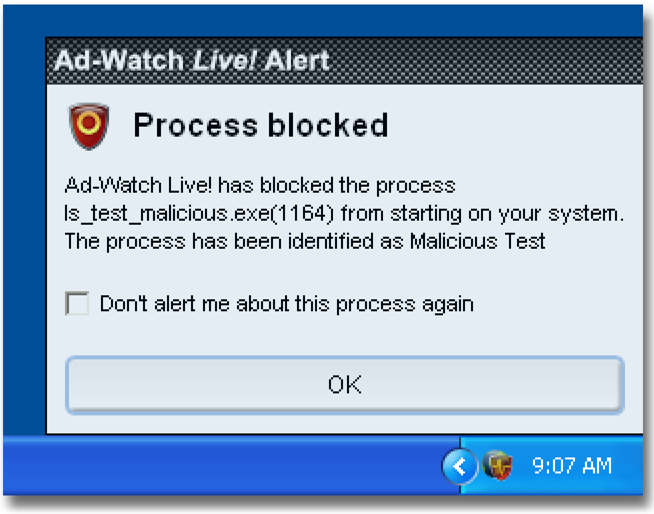
Exit Ad-Aware

Exits the Ad-Aware program completely.

Notifications

Process Notification

Ad-Watch *Live*! Process Notification



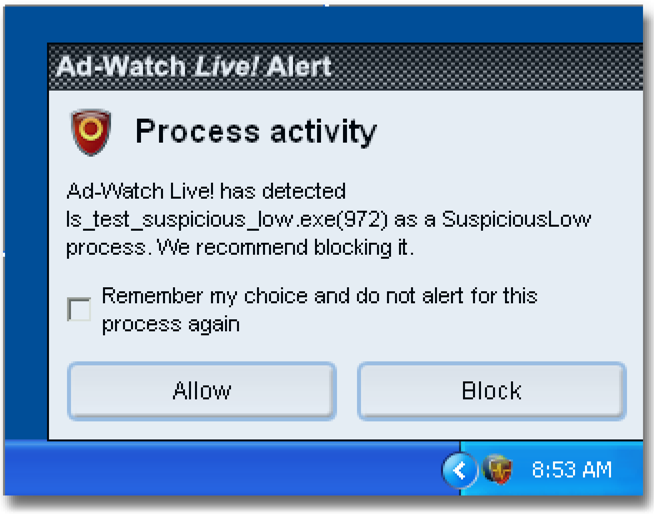
Ad-Watch *Live!* Alert

Process blocked

Ad-Watch Live! has blocked the process ls_test_malicious.exe(1164) from starting on your system. The process has been identified as Malicious Test

□ Don't alert me about this process again

When any malicious process starts on your computer, an 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.



Ad-Watch *Live!* Alert

Process activity

Ad-Watch Live! has detected ls_test_suspicious_low.exe(972) as a SuspiciousLow process. We recommend blocking it.

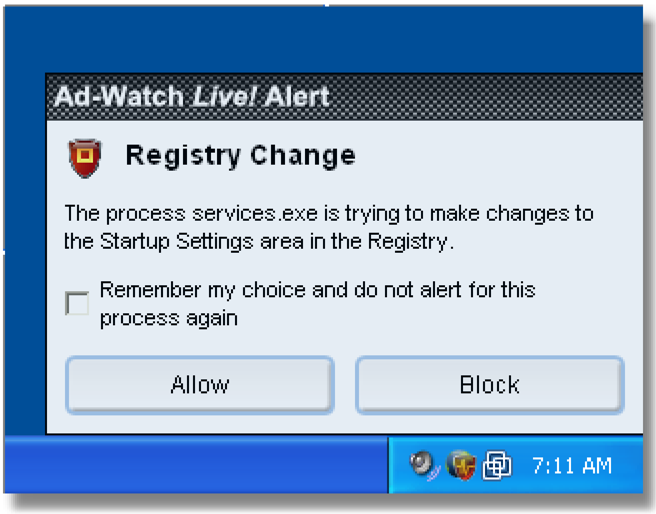
□ Remember my choice and do not alert for this process again

When any suspicious process starts on your computer, an 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.

Registry Notification

Ad-Watch *Live*! Registry Notification



Ad-Watch *Live!* Alert

Registry Change

The process services.exe is trying to make changes to the Startup Settings area in the Registry.

□ Remember my choice and do not alert for this process again

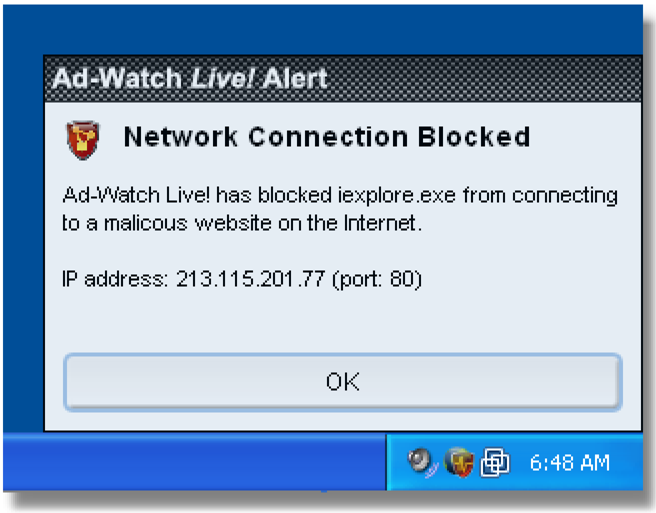
When any application makes a change your computer's registry, an Ad-Watch *Live!* notification window will appear and you will be given the choice to 'Allow' or 'Block' this registry change. Click 'Allow' and the process will be allowed to run. Warning! Only use this action if you are sure that the process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

Network Notification

Ad-Watch *Live*! Network Notification



Ad-Watch *Live!* Alert

Network Connection Blocked

Ad-Watch Live! has blocked iexplore.exe from connecting to a malicous website on the Internet.

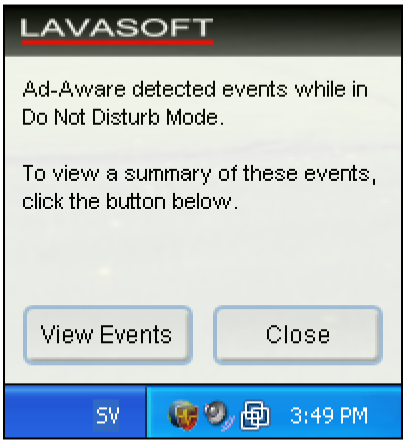
IP address: 213.115.201.77 (port: 80)

When any application tries to connect to a blacklisted IP address that is detected as malicious, an 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.

Events During Do Not Disturb Mode

When Ad-Aware exits Do Not Disturb Mode and events (RP alerts, scheduled scans, updates, etc.) have occurred while in Do Not Disturb Mode, this notification window will appear.

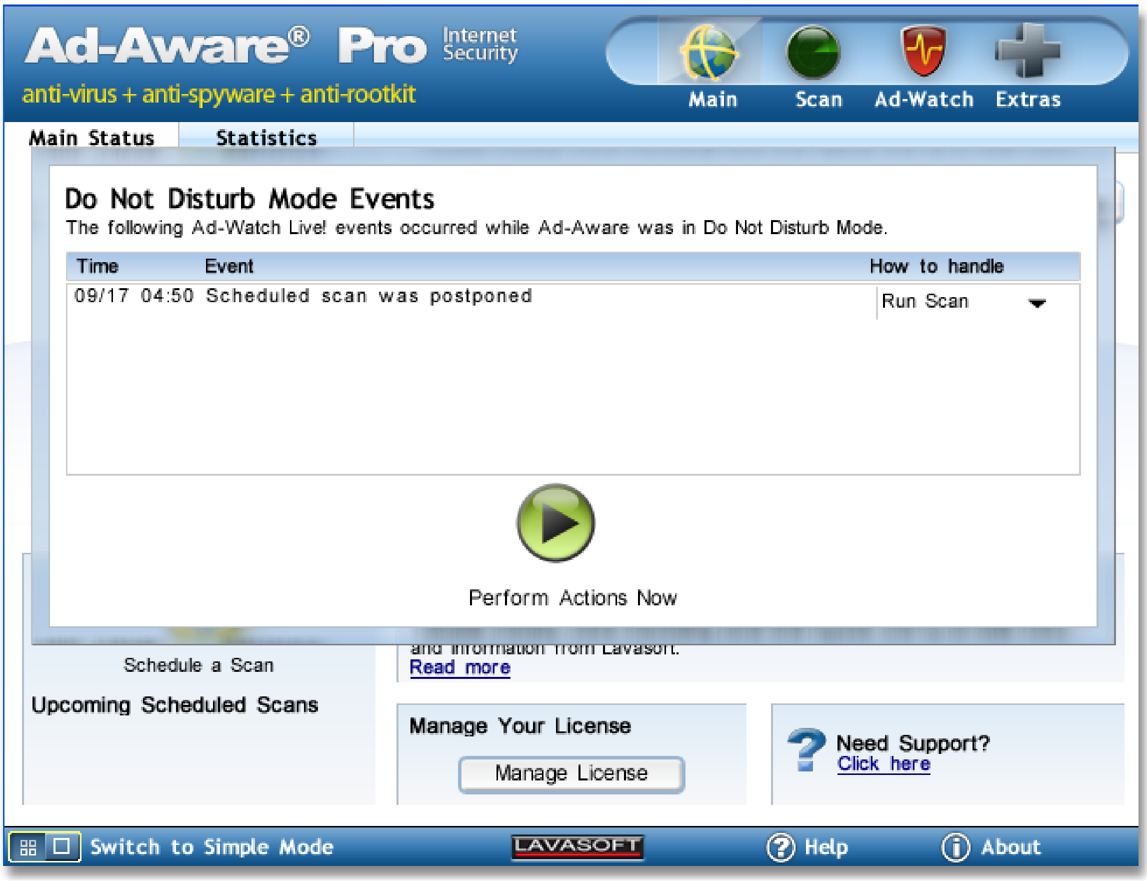


Ad-Aware detected events while in Do Not Disturb Mode.

To view a summary of these events, click the button below.

Click this notification to open the Summary of Events that have occurred while in Do Not Disturb Mode.

In the "Summary of Events" screen, events are grouped by the time they occurred, the event description and how these events are handled (action).
To change the required action from the "How to handle" list, choose the required action form the drop-down list and click "Perform Actions Now".
Ad-Aware will apply the required action for each detected event, and this action is applied if this event occurs again.



Do Not Disturb Mode Events

The following Ad-Watch Live! events occurred while Ad-Aware was in Do Not Disturb Mode.

Time	Event	How to handle
09/17 04:50	Scheduled scan was postponed	Run Scan

Perform Actions Now

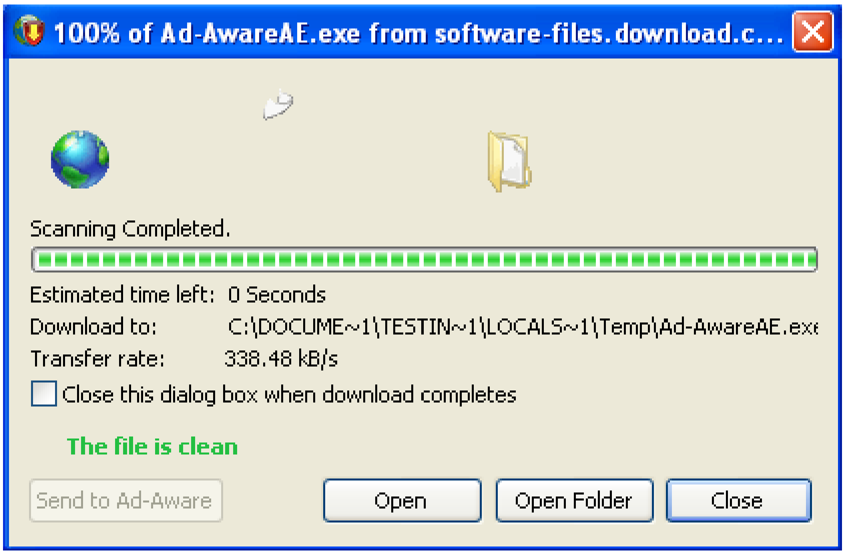
Download Guard for Internet Explorer

Download Guard for Internet Explorer provides an additional layer of protection that lets you download files on Internet Explorer confidently. If the file is malicious, you will simply be notified during the download process so that you can take action before any malware can infiltrate your system.

During the installation of Ad-Aware, you can choose to install Download Guard for Internet Explorer by ticking the option in the custom installation.
To complete the installation of Download Guard for Internet Explorer, after Ad-Aware has been installed, run the setup file and follow the installation wizard by clicking on Start->All Programs->Lavasoft->Install Download Guard for Internet Explorer.

No Malware Found Screen

If "Open" was selected in the download manager screen, the file opens. If the "Close this dialog box when download completes" checkbox is checked, the dialog will close.



100% of Ad-AwareAE.exe from software-files.download.c...

Scanning Completed.

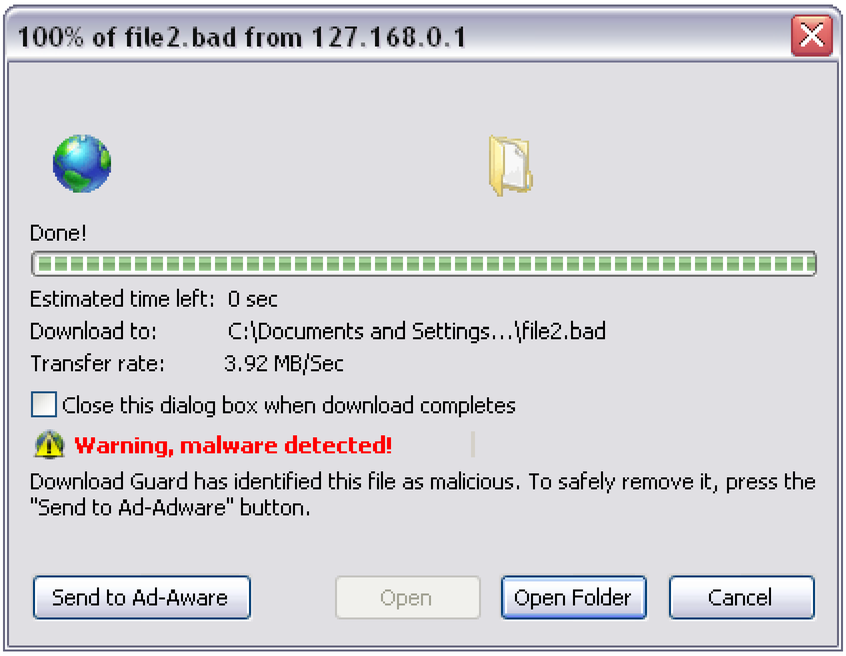
Estimated time left: 0 Seconds
Download to: C:\DOCUME~1\TESTIN~1\LOCALS~1\Temp\Ad-AwareAE.exe
Transfer rate: 338.48 kB/s

□ Close this dialog box when download completes

The file is clean

Warning Malware Detected Screen

This warning indicates that the file contains malware. The "Open" button is not enabled. We recommended that you press the "Send to Ad-Aware" button in order to let Ad-Aware handle the file and safely remove it. Even if the "Close this dialog box when download completes" checkbox is checked, the dialog will not close in order to ensure that you are aware of the infection.



100% of file2.bad from 127.168.0.1

Done!

Estimated time left: 0 sec
Download to: C:\Documents and Settings...\file2.bad
Transfer rate: 3.92 MB/Sec

□ Close this dialog box when download completes

Warning, malware detected!

Download Guard has identified this file as malicious. To safely remove it, press the "Send to Ad-Adware" button.

Uninstall Download Guard for Internet Explorer.

You can follow the steps below to uninstall Download Guard for Internet Explorer.

1. Go to the Control Panel.
2. Run "Add or Remove Programs".
3. Select Download Guard for Internet Explorer in the list and click the "Remove" button.
4. Verify uninstalling by selecting "Uninstall."
5. Download Guard for Internet Explorer will be uninstalled from your computer.

Using Ad-Aware's Public API

Ad-Aware Public API Information for Developers

Note! This information is intended for developers who wish to develop and share plug-ins for Ad-Aware.

In a similar spirit to the Community Translations Project, we are giving developers the chance to create their very own plug-ins for Ad-Aware. To upload plug-ins, sign-up to the MyLavasoft community at www.lavasoft.com, go to the plug-ins page, and join in the fun!

Details for Developers

- Ad-Aware can only have one scan in progress at a time. If the scan method is called while Ad-Aware is busy, the scan is ignored. Applications will have to implement some sort of queue mechanism themselves to handle this issue.
- In order to clean an infected file, a GUI scan must be performed. This is the same as manually scanning the file using Ad-Aware.
- Applications will need to locate "aawapi.dll" and load it. This file can be found in the "...\Lavasoft\Ad-Aware\" folder. This file should not be moved. Currently, this path cannot be found in the Windows registry (due to various reasons).
- Avoid disconnecting if a "scan" or "GUI scan" operation is being performed.
- All relative paths will be converted to absolute paths with environment path of the running application as its base. See GetFullPathName as a reference.
- AAW-API is thread safe, so every thread (and process) can connect and disconnect independently of each other without any interference, except that only one scan can be performed at any one time.

API
Flags (adaware_flag_e)

- ADAWARE_NO_FLAGS = 0,

- ADAWARE_AUTO_START = 1,

  Tries to start the service if unable to connect

Description: Use OR (|) to combine flags

Results (adaware_res_e)

- ADAWARE_SUCCESS = 0
  - The request was successful
- ADAWARE_UNABLE_TO_CONNECT
  - For some reason, aawapi can not establish a connection to Ad-Aware
- ADAWARE_NO_SUCH_FILE
  - Trying to scan a none existing file or directory
- ADAWARE_SCAN_FAILED
  - The scan did not successfully complete, discard the returned result
- ADAWARE_NOT_CONNECTED
  - Trying to use a method without a succeeding call to adaware_connect
- ADAWARE_ALREADY_CONNECTED
  - Trying to establish a new connection without closing the first (see adaware_disconnect)
- ADAWARE_BUSY
  - Ad-Aware is currently busy and can't scan your requested file

- ADAWARE_LAUNCH_GUI_FAILED
  - The gui couldn't be started
- ADAWARE_NOT_FOUND
  - Ad-Aware doesn't seem to be installed, can happen in the aawapi.dll isn't in the Ad-Aware folder or that an old version of Ad-Aware is installed.

Timeouts (adaware_timeout_e)

- ADAWARE_CONNECT_SINGLE_TRY_TIMEOUT = 0,
- ADAWARE_CONNECT_DEFAULT_TIMEOUT = 30000

Scan result

```
    typedef struct {
    wchar_t path[1024];                  //path of infected file
    wchar_t category[256];               //category of infection
    wchar_t family_name[256];            //name of the infection family
    wchar_t family_description[2048];    //description of the infection family
    adaware_infection_type infection_type;   //type of infection
    int TAI;                         //threat assessment index: 0 < TAI <= 10 if infection found
  } adaware_scan_results_t ;
```

Functions

adaware_res_e adaware_connect(adaware_flag_e, DWORD timeoutMs)

Description: Starts a connection to the Ad-Aware service, has to be called before any other adaware functions. It should never be called when a connection is already in place. timeoutMs is the connection timeout in milliseconds, a value smaller than or equal to 0 defaults to ADAWARE_CONNECT_DEFAULT_TIMEOUT.

Parameters: ADAWARE_NO_FLAGS, ADAWARE_AUTO_START

Return codes: ADAWARE_SUCCESS, ADAWARE_UNABLE_TO_CONNECT, ADAWARE_NOT_FOUND, ADAWARE_ALREADY_CONNECTED

Example:

```
adaware_res_e res = adaware_connect(ADAWARE_NO_FLAGS, 20000); //20
second timeout
```

or

```
adaware_res_e res = adaware_connect(ADAWARE_AUTO_START, 1000); //1
second timeout, start ad-aware if needed
```

adaware_res_e adaware_disconnect(adaware_flag_e)

Description: Closes the connection to the adaware service.

Parameters: ADAWARE_NO_FLAGS

Return codes: ADAWARE_SUCCESS, ADAWARE_NOT_CONNECTED

Example:

```
adaware_res_e res = adaware_discconnect(ADAWARE_NO_FLAGS);
```

adaware_res_e adaware_scan_file(const wchar_t *filepath, adaware_scan_result_t &result, int &malicious)

Description: Scans a given file and populate result with useful data.

Note: Malicious is either 0 or 1, but we are using an int instead of a bool to provide C compatibility. If adaware_scan_file doesn't return ADAWARE_SUCCESS, the data in result will be undefined.

Return codes: ADAWARE_SUCCESS, ADAWARE_NOT_CONNECTED, ADAWARE_NO_SUCH_FILE, ADAWARE_SCAN_FAILED,

Example:

```
adaware_scan_result_t scanres;
```

```
int malicious;

adaware_res_e res = adaware_scan_file(L"pathtofile", &scanres, ADAWARE_NO_FLAGS,
&malicious);

if(res == ADAWARE_SUCCESS) {
 //do something with the scanres data
}
```

adaware_res_e adaware_scan_file_with_gui(const wchar_t *filepath)

Description: Scans a given file or directory with the adware gui. The caller will not access the scan results. This is currently the only way to let Ad-Aware handle (remove) any infections.

Return codes: ADAWARE_SUCCESS, ADAWARE_NOT_CONNECTED, ADAWARE_BUSY, ADAWARE_LAUNCH_GUI_FAILED

Example:

```
adaware_res_e res = adaware_scan_file_with_gui(L"pathtofile");
```

adaware_res_e adaware_is_busy()

Description: Check if any scan is currently in progress

Return codes: ADAWARE_SUCCESS, ADAWARE_NOT_CONNECTED, ADAWARE_BUSY

Example:

```
adaware_res_e res = adaware_scan_file_with_gui(L"pathtofile");
if(res == ADAWARE_BUSY) {
  // then we should "wait" until next scan
}
```

void adaware_set_mock(void *config) (not public)

Description: Replaces the service connection with a mock object with the given config, only for testing purposes.

Example:

```
ServiceClientMockConfig *mock = new ServiceClientMockConfig();
mock->canConnect = false;

mock->canAutoStart = true;
adaware_set_mock(mock);
//run test
```

API Samples

Two API sample applications: File scanner and CMD Test Application.

File scanner sample

Description: A simple test application demonstrating the basic functionality of the Lavasoft Ad-Aware API.

Files: file_scanner_sample.cpp

Usage: <appname>.exe AAWPath file_to_scan

AAWPath: The Ad-Aware install directory.
file_to_scan: Path to the file to be scanned.

Code:

```
/*

//	file_scanner_sample.cpp
```

```
//
//          Description:      A simple test application demonstrating the basic functionality
//                                                  of the Lavasoft Ad-Aware API
//
//          Remarks:                    Make sure that aawapi.dll is located in your Ad-Aware directory
//
//          Usage:                      <appname>.exe AAWPath file_to_scan
//
//          Authors:                    Anders Olofsson and Simon Edwardsson
*/
#include <windows.h>
#include <iostream>
/* include the Ad-Aware api for all the exported functionality */
#include "Ad-AwareAPI.h"
/*
Functor typedefs for Ad-Aware,
see the documentation for all exported functions
*/
typedef adaware_res_e (WINAPI* adaware_connect_cbp)(adaware_flag_e, signed int);
typedef adaware_res_e (WINAPI* adaware_disconnect_cbp)(adaware_flag_e);
typedef adaware_res_e (WINAPI* adaware_scan_file_cbp)(const wchar_t*,
adaware_scan_results_t *, int *);
/* Making the functor pointers global */
adaware_connect_cbp _adaware_connect;
adaware_disconnect_cbp _adaware_disconnect;
adaware_scan_file_cbp _adaware_scan_file;
/* Holds the API dll */
HINSTANCE hDLL;
/* Result messages (for debugging) */
wchar_t *resCodes[] =  {L"ADAWARE_SUCCESS",
          L"ADAWARE_UNABLE_TO_CONNECT",
          L"ADAWARE_NO_SUCH_FILE",
        L"ADAWARE_SCAN_FAILED",

        L"ADAWARE_NOT_CONNECTED",

        L"ADAWARE_ALREADY_CONNECTED",

        L"ADAWARE_BUSY",

        L"ADAWARE_LAUNCH_GUI_FAILED",

        L"ADAWARE_NOT_FOUND"};

/*  Initializes the functor pointers

Returns 0 upon success */

int Init(std::wstring &path)
{
        std::wstring dll_path = path;
        dll_path += L"\\";
        dll_path += L"aawapi.dll";

        /* Load API dll */
        hDLL = LoadLibraryW(dll_path.c_str());

        /* If Load was successful */
        if (hDLL != NULL)
        {
                /* Get function adresses: */

                _adaware_connect = (adaware_connect_cbp)GetProcAddress(hDLL,
                                                                "adaware_connect");

                _adaware_disconnect = (adaware_disconnect_cbp)GetProcAddress(hDLL,
                                                                "adaware_disconnect");

                _adaware_scan_file = (adaware_scan_file_cbp)GetProcAddress(hDLL,
                                                                "adaware_scan_file");

                /* If anything failed */
                if (!_adaware_connect || !_adaware_disconnect || !_adaware_scan_file)
                {
                        std::wcout<<L"FATAL: error occured while loading library function" <<
std::endl;

                        FreeLibrary(hDLL);
                        return 1;
                }
        }
        else /* Failed loading dll */
        {

                std::wcout << "FATAL: could not load awwapi.dll, sorry" << std::endl;
                return 1;
        }

        return 0;
}

void usage()
{
        std::cout << "usage: example_app.exe path_to_adaware file_to_scan" << std::endl;
}
```

```
int wmain(int argc, wchar_t* argv[])
{

    if(argc < 3)
    {
        usage();
        return EXIT_FAILURE;
    }

    std::wstring aaw_path    = argv[1];
    std::wstring file_path   = argv[2];

    /* Initialization */
    int initRes = Init(aaw_path);

    if(initRes != 0)
        return EXIT_FAILURE;

/*

    Connect and print result

    If Ad-Aware is not started, it will autostart.

*/

    int connectRes = _adaware_connect(ADAWARE_AUTO_START,
ADAWARE_CONNECT_DEFAULT_TIMEOUT);
    std::wcout<<L"adaware_connect: "<<resCodes[connectRes]<<std::endl;

    /* Scan and print result */

    adaware_scan_results_t scanResult;

    int infection;

    int scanRes = _adaware_scan_file(file_path.c_str(), &scanResult, &infection);
    std::wcout<<L"adaware_scan_file: "<<resCodes[scanRes]<<std::endl;

    /* If infection, print type */

    if(infection != 0)
        std::wcout<<L"Infection found! Family name: "<<scanResult.family_name<<std::
endl;
    else
        std::wcout<<L"No infections found"<<std::endl;

    wprintf(L"infection: %d\n", infection);

    /* Disconnect and print result */

    int disconnectRes = _adaware_disconnect(ADAWARE_NO_FLAGS);
    std::wcout<<L"adaware_disconnect: "<<resCodes[disconnectRes]<<std::endl;

    /* Free dll */

    FreeLibrary(hDLL);
    return EXIT_SUCCESS;

}
```

CMD Test Application

Description: An extended sample application capable of scanning files and folders, using both GUI scan and normal scan.

Files: CMDTestApplication.cpp

Usage: <appname>.exe AAWPath action [files]
AAWPath: The Ad-Aware install directory.
action:
/scan [filepaths] scan files and print results
/scandir [folderpath] scans the directory recursively
/scangui [path] scans the file or folder with the AAW GUI
Example: CMDTestApplication.exe "C:\Program Files\Lavasoft\Ad-Aware\ /scan "C:\file.txt"

Code:

```
/*
//    CMDTestApplication.cpp
//
//    Description:    An extended test application demonstrating all the functionality
//                    of the Lavasoft Ad-Aware API
//
//    Remarks:        Make sure that aawapi.dll is located in your Ad-Aware directory
//
//    Usage:          <appname>.exe AAWPath action [files]
//
//                    AAWPath:    The Ad-Aware install directory.
//                    action:
//                            /scan [filepaths]       scan files and print results
//                            /scandir [folderpath]   scans the directory recursively
//                            /scangui [path]         scans the file or folder with the AAW GUI
//
//                    Example: CMDTestApplication.exe "C:\Program Files\Lavasoft\Ad-Aware\ /scan "C:
\file.txt"
//
//    Authors:        Anders Olofsson and Simon Edwardsson
*/

#include "Ad-AwareAPI.h"
#include <iostream>
#include <windows.h>
#include <stdio.h>
#include <tchar.h>

/* first of we create some callbacks for our dll functions */
typedef adaware_res_e (WINAPI* adaware_connect_cbp)(adaware_flag_e, signed int);
typedef adaware_res_e (WINAPI* adaware_disconnect_cbp)(adaware_flag_e);
typedef adaware_res_e (WINAPI* adaware_scan_file_cbp)(const wchar_t*,
adaware_scan_results_t *, int *);
typedef adaware_res_e (WINAPI* adaware_scan_file_with_gui_cbp)(const wchar_t*);

/* if you want to call adaware_connect you will now write _adaware_connect(); */
adaware_connect_cbp _adaware_connect;
adaware_disconnect_cbp _adaware_disconnect;
adaware_scan_file_cbp _adaware_scan_file;
adaware_scan_file_with_gui_cbp _adaware_scan_file_with_gui;

/* this is our function for scaning a file, dealing with the result and possible errors */
int scan_action(wchar_t *file) {
   wprintf(L"Begin scanning \"%s\"...\n",file);
```

```
    /* scan the file */
    adaware_scan_results_t scan_result;
    int found;
    int res = _adaware_scan_file(file, &scan_result, &found);

    /* if scan did not succeed:*/
    if(ADAWARE_SUCCESS != res) {
        switch(res) {
            case ADAWARE_NO_SUCH_FILE:
                wprintf(L"Can not locate (maybe a directory?): \"%s\"\n", file);
                break;
            default:
                wprintf(L"Scanning failed, error code: %i\n", res);
                break;
        }
    } else { /*scan succeded */
        /* is there anything to report? please note that scan_result is undefined if found is false */
        if(found) {
            wprintf(L"Path: %s\nInfection type: %i\n", scan_result.path, scan_result.infection_type);
            wprintf(L"Familyname: %s\nThreatlevel: %i\n", scan_result.family_name, scan_result.TAI);
            wprintf(L"Category: %s\nFaimlyDescription: %s\n", scan_result.category, scan_result.
family_description);
        } else {
            wprintf(L"\"%s\" seems to be clean\n", file);
        }

    }

    return 0;
}

/* scans a directory recursively. Call with depth = 0*/
void scan_dir(const wchar_t *filepath, int depth) {
        /* don't scan more than 20 directories recursively*/
        if(depth > 20)
            return;

        WIN32_FIND_DATA findFileData;
        HANDLE hFind;

        /* scan the provided directory */
        wchar_t *tmp = new wchar_t[wcslen(filepath) + wcslen(L"/* ")];
        wsprintf(tmp, L"%s\\*", filepath);
        hFind = FindFirstFile(tmp, &findFileData);
        delete[] tmp;

        if(hFind  == INVALID_HANDLE_VALUE) {
            wprintf(L"No file(s) found\n");
            return;
        }

        if(depth == 0) {
            /* init the adaware connection */
            int res = _adaware_connect(ADAWARE_NO_FLAGS, -1);
            if(ADAWARE_SUCCESS != res) {
                printf("FATAL: Could not connect to adaware (%i)\n", res);
                return;
            }
        }

        do {
            /* we do not care about . and .. since they are no real files */
            if(!wcscmp(findFileData.cFileName,L".") || !wcscmp(findFileData.cFileName, L".."))
                continue;

            /* if file is a directory: */
            if(findFileData.dwFileAttributes == FILE_ATTRIBUTE_DIRECTORY) {
                wchar_t *tmp = new wchar_t[wcslen(filepath) + wcslen(L"\\ ") + wcslen(findFileData.
cFileName)];
                wsprintf(tmp, L"%s\\%s", filepath, findFileData.cFileName);
                /* recursive scan */
                scan_dir(tmp, depth + 1);
                continue;
            }

            /* not a directory, scan this file */
            wchar_t *tmp = new wchar_t[wcslen(filepath) + wcslen(L"\\ ") + wcslen(findFileData.
cFileName)];
            wsprintf(tmp, L"%s\\%s", filepath,findFileData.cFileName);
            scan_action(tmp);
            delete[] tmp;
            wprintf(L"+-------------------------------+\n");

            /* loop as long as there are files left*/
        } while(FindNextFile(hFind, &findFileData));

        if(depth == 0) {
            /* destroy the connection */
            _adaware_disconnect(ADAWARE_NO_FLAGS);
        }
}

/* scans the specified file or directory using the Ad-Aware GUI*/
int scan_with_gui(const wchar_t *path)
{
    /* init the adaware connection */
    int res = _adaware_connect(ADAWARE_NO_FLAGS, -1);
    if(ADAWARE_SUCCESS != res) {
        printf("FATAL: Could not connect to adaware (%i)\n", res);
        return 0;
    }

    /* scan path with gui*/
    res = _adaware_scan_file_with_gui(path);

    if(res == ADAWARE_BUSY)
        std::wcout << L"Ad-aware is currently busy, please try again later" << std::endl;
    else if(res != ADAWARE_SUCCESS)
        std::wcout << L"Scanning failed" << std::endl;

    /* destroy the connection */
    _adaware_disconnect(ADAWARE_NO_FLAGS);
    return 0;
};

/* prints how the application should be used */
int usage(wchar_t *app) {
    wprintf(L"Usage:\t%s AAWPath action [files]\n\n"
            L"\tAAWPath:\n"
            L"\t\t[Ad-Aware install directory]\n"
            L"\taction:\n"
            L"\t\t/scan [filepath]\tscan file and print results\n"
            L"\t\t/scandir [filepath]\tscan all files in filepath directory and print results\n"
            L"\t\t/scangui [filepath]\tscan a file using the Ad-Aware GUI",
            app, app);
    return 0;
}

/* main function */
int wmain(int argc, wchar_t* argv[])
{
    /* parse and handle input: */
    wchar_t *action = 0;
    wchar_t *options[10];
    int nr_options = 0;
    for(int i = 1; i < argc; i++)
    {
        if(argv[i][0] == '/')
            action = argv[i];
        else
        {
            /* no more than 10 arguments to a command! */
            if(i > 2 && nr_options < 10)
                options[nr_options++] = argv[i];
        }
    }

    /* we have to specify an action */
    if(!action) {
        return usage(argv[0]);
    }
    /* Load the dll */
    std::wstring aawpath = argv[1];
    aawpath.append(L"\\aawapi.dll");
    HINSTANCE hDLL = LoadLibraryW(aawpath.c_str());
    wprintf(L"Path to dll: \t%s\n", aawpath.c_str());

    if (hDLL != NULL)
    {
        /* then we load the functions */
        _adaware_connect = (adaware_connect_cbp)GetProcAddress(hDLL,
                                               "adaware_connect");
        _adaware_disconnect = (adaware_disconnect_cbp)GetProcAddress(hDLL,
                                               "adaware_disconnect");
        _adaware_scan_file = (adaware_scan_file_cbp)GetProcAddress(hDLL,
                                               "adaware_scan_file");
        _adaware_scan_file_with_gui = (adaware_scan_file_with_gui_cbp)GetProcAddress(hDLL,
                                               "adaware_scan_file_with_gui");
        /* If anything failed */
        if (!_adaware_connect || !_adaware_disconnect || !_adaware_scan_file || !
_adaware_scan_file_with_gui)
        {
            std::wcout << "FATAL: error occured while loading library function" << std::endl;
            std::cout << (int)(_adaware_connect) << (int)(_adaware_disconnect) << (int)
_adaware_scan_file << std::endl;
            FreeLibrary(hDLL);
            return 1;
        }
    } else {
        std::wcout << "FATAL: could not load awwapi.dll, sorry" << std::endl;
        return 1;
    }

    /* ACTION: SCAN DIRECTORY */
    if(!wcscmp(action, L"/scandir"))
    {

        if(nr_options != 1)
        {
            wprintf(L"scandir needs exactly one argument");
            return 1;
        }
        //wprintf(L"options: %d\n", nr_options);
        scan_dir(options[0], 0);
    }
    /* ACTION: SCAN WITH GUI */
    else if(!wcscmp(action, L"/scangui"))
    {
        if(nr_options != 1)
        {
            wprintf(L"/scangui needs exactly one argument\n");
            return 1;
        }
        /* add path to a temp string*/
        std::wstring tmp = L"";
        tmp += options[0];
        /* scan file with gui */
        scan_with_gui(tmp.c_str());

    }
    /* ACTION: SCAN FILE(-S) */
    else if(!wcscmp(action, L"/scan"))
    {
        if(nr_options < 1)
        {
            wprintf(L"/scan needs at least one argument\n");
            return 1;
        }

        /* init the adaware connection (before the scans, rather than connecting once for each scan)
*/
        int res = _adaware_connect(ADAWARE_NO_FLAGS, 5000);
        if(ADAWARE_SUCCESS != res)
        {
            printf("FATAL: Could not connect to adaware (%i)\n",res);
            return 0;
        }
        /* make a scan for every file specified */
        for(int i = 0; i < nr_options; i++)
        {
            res = scan_action(options[i]);
        }
        /* destroy the connection */
        _adaware_disconnect(ADAWARE_NO_FLAGS);
        return 0;
    }
    else
    {
        /* default:  print usage*/
        return usage(argv[0]);
    }

    return EXIT_SUCCESS;
}
```

Using Command Line Parameters

Ad-Aware can be controlled by using command line parameters.

Ad-AwareCommand.exe

Ad-AwareCommand.exe is the command line interface to Ad-Aware. Ad-AwareCommand.exe runs in a command prompt window and executes the command. It returns data in two ways, first as the application executable exit code.
The exit codes are:

0 = Ok
1 = Run Error
3 = Connect to service failed
4 = Bad Input

The second return data is passed on standard output as XML. It will have a numeric code and in some cases text data. The "XML return codes" are numeric codes, these can be found in the XML in the 'result' node. The meaning of these codes are:

00 = Ok
01 = Failed to connect to service
02 = No license or activation code on system
03 = Application not licensed
04 = Could not register trial license
05 = Unrecognized parameter
06 = Not logged in as administrator
07 = Scan profile not found
08 = No server name passed

All XML return codes are not applicable for every command line parameter, possible XML return codes are listed under each command.

Example:

```
C:\>Ad-AwareCommand.exe scan myscanprofile manual
```

Ad-Aware will run in the command line window and perform the scan named 'myscanprofile' with manual cleaning.

Command line Parameters

scan
Description: Starts a scan
Parameters: <full/smart/profile> [manual]
profile - Which scan profile to use. Use quotes if there is a space in the profile name e.g. "my scanprofile".
manual - This is an optional parameter used when you want to manually choose the cleaning actions.
When the scan is completed and if an infection is found 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.

Possible XML return codes: 00,01,07

Example:

```
C:\>Ad-AwareCommand.exe scan myscanprofile manual
C:\>Ad-AwareCommand.exe scan smart
```

update all
Description: Updates the software and definitions files.
Parameters: [silent]

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

Possible XML return codes: none

Example:
```
C:\>Ad-AwareCommand.exe update all silent
C:\>Ad-AwareCommand.exe update all
```

license
Description: Registers the product with a specified serial number.
Parameters: [trial] <code>

Possible XML return codes: 00,01,02,03,04,05

Example:
```
C:\>Ad-AwareCommand.exe license 12345-ABCD-14AC4-95784
```

get-hardware-fingerprint
Description: Reads the hardware fingerprint.
Parameters:

Possible XML return codes: 00,01

Example:
```
C:\>Ad-AwareCommand.exe get-hardware-fingerprint
```

set-update-server
Description: Changes which update server to use for software updates.
Parameters: <servername>

Possible XML return codes: 00,08

Example:
```
C:\>Ad-AwareCommand.exe set-update-server mynewserver.com
```

get-license-info
Description: This parameter retrieves the license information.
Parameters:

Possible XML return codes: 00,01

Example:
```
C:\>Ad-AwareCommand.exe get-license-info
```

get-reports
Description: Retrieves scan or realtime protection reports.
Parameters: <scan/rp>

Possible XML return codes: 00,01,05

Example:
```
C:\>Ad-AwareCommand.exe get-reports rp
```

get-settings

Description: Retrieves the current settings.
Parameters:

Possible XML return codes: 00

Example:

```
C:\>Ad-AwareCommand.exe get-settings
```

set-settings
Description: Sets the settings.
The settings are passed as XML to standard input.
Parameters:

Possible XML return codes: 00,01

Example:

```
C:\>Ad-AwareCommand.exe set-settings
```

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.