Ad-Aware SE

Professional edition

Manual

v 1.04

Table of Contents

Part I What is Ad-Aware SE? 3

1 What's new in Ad-Aware SE? ... 3

2 System Requirements ... 4

Part II Getting started 6

1 How to download ... 6

2 Install Ad-Aware SE ... 6

3 Performing your first scan ... 7

4 Stay protected - set up automation ... 7

Part III Uninstall Ad-Aware SE 9

1 Uninstaller ... 9

2 Control Panel ... 9

Part IV The Ad-Aware Interface 10

1 Main Status screen ... 11

2 Preparing System Scan ... 11

3 Performing System Scan ... 13

4 Scan Complete ... 14

5 Scanning Results ... 15

- Scan Summary ... 15
- Critical Objects ... 16
- Negligible Objects ... 19
- Scan Log ... 21

6 Ignore list ... 22

7 Quarantined Objects ... 24

8 WebUpdate ... 25

- Performing WebUpdate... main screen ... 25
- WebUpdate Configuration screen ... 26
- WebUpdate process completed ... 27

9 Add-ons ... 27

- Tools ... 27
- Extensions ... 28
- Statistics ... 29

10 Settings ... 31

- General Settings ... 32
- Scan Settings ... 33
- Advanced Settings ... 34
- Startup Settings ... 35
- Default Settings ... 37
- Interface Settings ... 38
- Tweak Settings ... 39

Part V Using Ad-Aware SE 45

1 Update the definition file ... 45
2 Using Command Line Parameters ... 46
3 Change language ... 48
4 Changing Ad-Aware SE's skin ... 48
5 What is the quarantine? ... 48
6 What is the ignore list? ... 49
7 Setting up Ad-Aware SE ... 50
8 Performing your first scan ... 50
9 Automated scans ... 51
10 Virus warnings while performing a scan with Ad-Aware ... 52

Part VI What are add-ons? 53

1 Download, install & run add-ons ... 53
2 How to uninstall Add-ons for Ad-Aware SE ... 54

Part VII What is Ad-Watch? 55

1 Ad-Watch Event Log ... 55
2 Tools & Preferences ... 56
Options ... 58
Rule Editor ... 59
Add New Rule ... 60
Filter ... 61
Pop-ups ... 62
Statistics ... 63

Part VIII What is Process-Watch? 64

1 The Interface ... 64

Part IX Purchasing additional solutions from Lavasoft 67

Part X Support 68

1 Support Forums ... 68
Support Forums FAQ ... 68
2 Knowledge Base ... 69
3 Threat Assessment Chart - TAC ... 70

Index 72

1 What is Ad-Aware SE?

Ad-Aware SE is the latest version of our award winning and industry leading line of antispyware solutions and represents the next generation in Spyware detection and removal. It is quite simply the most advanced solution available to protect your privacy. With the all new Code Sequence Identification (CSI) technology that we have developed, you will not only be protected from know content, but will also have advanced protection against many of their unknown variants.

Designed for Windows 98, 98SE, Win ME, Win NT 4, Win 2000, and Win XP Home/Professional you can be sure that you will have the most effective privacy protection that has ever been offered by Lavasoft. Ad-Aware SE Professional edition will comprehensively scan your memory, registry, hard, removable and optical drives for known Data-mining, aggressive advertising, Parasites, Scumware, selected Keyloggers, selected traditional Trojans, Dialers, Malware, Browser hijackers, and tracking components.

See the What's new in Ad-Aware SE? chapter for a detailed description of the improvements we have built into our latest version of Professional.

1.1 What's new in Ad-Aware SE?

New command line parameters that allow for silent and automated operation of Ad-Aware

UNC support for remote storage of Preferences, definitions, and log files

New results screens and detailed statistics

Improved logging and reporting

Hardened against third party uninstall with encrypted preference files

Links to more information on detected content from our website

New safety option that allows you to write protect sensitive system files such as the Hosts file

Scanning engine improvements
- Extended protection against DLL-injection, SE can unload process modules on the fly
- Extended Memory scanning
- Now scans all modules loaded by a process
- Uses our all new CSI (Code Sequence Identification) technology to identify new and unknown variants of known targets

Extended Registry scanning
- Now scans registry branches of multiple user accounts
- Performs additional smart checks to detect dynamically created references
- Scanning speed noticeably faster
- Extended Scanning for known and unknown/possible Browser-Hijackers

Extended Disk scanning
- Now scans and lists alternate Data-streams on NTFS volumes
- Now Ad-Aware supports scanning of Cabinet files, (including spanned archives)
- Scanning speed increased
- Improved Hosts-file scan
- Now Ad-Aware and Ad-Watch Use much smaller reference files

Several User Interface improvements
- Improved Graphical UI
- Ad-Aware now supports custom graphical Skins
- More user friendly Plug-in/Extension GUI (Plug-ins and Extensions now shown on separate screens)

- New Scan Result view, Includes a scan summary and Detailed view
- Ad-Aware now linked to the online TAC database

Multiple New Tweak options
- Unloading of process modules during a scan
- Obtaining command line of scanned processes
- Ignoring spanned cab files
- Scan registry for all users instead of current user only
- Permanent archive caching
- Always try to unload modules before deletion
- Disable manual quarantine if auto quarantine is selected
- Block pop-ups aggressively
- Load Ad-Watch minimized
- Hide Ad-Watch tray icon
- Write protect system files after repair
- Limit drive selection to fixed drives
- Use gridlines in item lists
- Log file detail section condensed

Process-Watch
- Improved Process-Watch scanning capabilities and scanning speed (Using the new fingerprint engine)
- Several Process-Watch Interface improvements
- Option to create a Hexdump of the process memory or dump the process memory to disk

Several logfile improvements
- Includes support for separate removal logfiles
- Allows adding a Reference summary/index to log files
- Logfile contains overall more detailed information

Ad-Watch
- Several GUI improvements
- Ad-Watch now supports Cookie Blocking
- Site-manager to edit the popup-blacklist included
- Ad-Watch now uses the new CSI technology to detect new and unknown variants of known targets
- New Ad-Watch configuration screen
- New rules editor for pre-defined blocking exclusions
- Support for hiding the Ad-Watch tray icon for unattended operation

1.2 System Requirements

Processor: P166

RAM: Operating system + 24 MB

Hard Disk: 25 MB free space (minimal configuration)

Operating Systems:
Windows 98
Windows 98se
Windows Me
Windows NT4 Workstation
Windows NT4 Server
Windows 2000 Pro
Windows 2000 Server
Windows 2003 Server
Windows XP Home
Windows XP Pro

Windows XP (Home/Professional)
Windows XP 64-Bit Edition
Windows Terminal Services

Other: Internet Explorer version 5.5 or higher

2 Getting started

2.1 How to download

When you purchased Ad-Aware SE Professional you received an e-mail with a download link. Click on the link to start the download. A grey popup window will open up. The popup window is titled "**File Download**". Make sure that the File Name is "**aawsepro.exe**". Click on the "**Save**" button and select the folder "**My Documents**". Click "**Save**" again and the download will start.

2.2 Install Ad-Aware SE

If you are installing Ad-Aware on Windows NT, 2000, or XP, please ensure that you have administrative rights. Ad-Aware must be installed in an account that has adequate permissions to perform its function. If you are unsure if you have the requisite permissions please contact your system administrator or refer to your computer's user guide before proceeding.

1. **Start installation**
   When the download is completed, go to "**My Documents**" and double-click on the "**aawsepro.exe**" file to start the installation.
2. **Welcome Screen**
   Press "**Next**" to continue to the license Agreement Screen
   Please read the license agreement before you proceed. When you have completed reviewing the agreement and if you agree to the terms, click the checkbox next to "**I accept the license agreement**" and press "**Next**" to continue with the installation of the software.
3. **Uninstall previous versions of Ad-Aware**
   Ad-Aware SE may not function correctly if old versions are not removed prior to installing a new version or an upgrade. To ensure proper installation and operation of Ad-Aware SE please make sure "**Yes, uninstall previous version of Ad-Aware. (Recommended)**" is selected and click "**Next**" to continue.
   a. **Ad-Aware Plug-in Uninstall pop-up**
      You might get a grey pop-up asking if you want to uninstall the plug-ins for the previous version of Ad-Aware. Click "**Yes**" to remove the old plug-ins and continue the uninstall process.
   b. **Select Uninstall method**
      Select "**Automatic**" and click "**Next**".
   c. **Perform Uninstall**
      Click finish to complete uninstalling your old version of Ad-Aware.
   d. **Uninstall Successful!**
      Click "**Next**" to continue with the installation of Ad-Aware SE Professional.
4. **Destination Location**
   Click "**Next**" to accept the default location or use "**Browse**" to specify where you want Ad-Aware SE Professional installed.
5. **Install to All Users menu**
   If you have multiple user accounts on your system choose "**Anyone who uses this computer**" and click "**Next**".
6. **Start Installation**
   Click "**Next**" to start installing Ad-Aware SE Professional onto your computer.After the copying of files you will get a confirmation that the installation was successful.
7. **Installation successful**
   Click "**Finish**" to complete the installation process. You now have the option to "**Update the definition file**", "**Run a full system scan**" and "**Open the help file now**".

2.3 Performing your first scan

Before you scan your computer with Ad-Aware SE for the first time you should run WebUpdate to make sure that you have the latest definition file. It is also recommended to have Ad-Aware set to automatically quarantine files prior to removal. Click on the "**Settings**" button (gear symbol in the upper right corner of the main status screen) in the quick launch toolbar to open the General settings screen. Check the "**Automatically quarantine objects prior to removal**" setting and then click "**Proceed**" to save your changes.

When this is done you are ready to perform your first scan. Click the "**Scan now**" button in the main menu on the left side of the main status screen or use the "**Start**" button in lower right corner. This will open the Preparing System Scan screen. Select "**Perform Full System scan**" and click "**Next**" to start your first scan.

After the scan is completed you will be presented with a detailed listing of the items that were detected. Please be sure to review each item that has been presented in the results screen before removing them. Ad-Aware is designed to report possible suspicious content present on your system and to allow you a simple method for removing it should you so decide. We do not suggest or recommend that everything detected by Ad-Aware should be removed; it is up to you the user to make that decision. We understand that this may be a difficult task; therefore we have developed TAC which stands for Threat Assessment Chart. More information is available in the Threat Assessment Chart - TAC chapter.

If you have decided to keep one or more items, select them from the scan results list (be sure to unselect other content you wish to remove) and right click the entry to open the context menu. Either select each item individually for each component to be ignored, or use the selection options in the context menu. Select the "**Add selection to ignore list**" to add this content to your ignore list. Ad-Aware will not display these items in the scan results when you perform scans in the future.

Once this content has been added to your ignore list you will be taken back to the scan results screen where you can repeat the above process as required, to not select anything more (all items are unchecked), or to remove the content as you deem appropriate.

Click the "**Next**" button on the Scan Complete screen to view the Scanning Results. Select the objects you want to remove by selecting them in the scan results lists or right click to select multiple items by using the context menu. Click "**Next**" and then "**OK**" in the pop-up window to confirm the removal.

2.4 Stay protected - set up automation

To keep your computer protected it is important that you update the definition file and run scans on a regular basis. You can set up Ad-Aware to automatically update the definition file, scan, quarantine detected objects and clean your computer on Windows startup. To set up the automation follow the step-by-step instructions below.

1. Click the "**Settings**" button in the toolbar and click the "**Startup**" button to go to the Startup Settings screen.

Automatic WebUpdate*

2. Select "**Automatically check for updated definitions on startup**" in the Auto-Updating section

Automatic Scans

3. Select a scan mode in the Startup Scan Mode section

Automatic Cleaning

4. Select "**Clean automatically**" in the Startup Action section

Automatic Quarantine

5. Click the "**General**" button to go to General Settings

6. Select "**Automatically quarantine objects prior to removal**" in the Safety Settings section
7. To save your changes click "**Proceed**".

* You must be connected to the Internet to update the definition file

3 Uninstall Ad-Aware SE

3.1 Uninstaller

1. Go to the "**Lavasoft Ad-Aware SE Professional**" folder in your Start menu
2. Run "**Uninstall Ad-Aware SE Professional**"
3. Select Uninstall Method
   Select "**Automatic**" and click "**Next**"
4. The uninstall of Ad-Aware SE Professional is completed when the program exits

3.2 Control Panel

1. Go to the Control Panel
2. Run "**Add or Remove Programs**"
3. Select Ad-Aware SE Professional in the list and click the "**Change/Remove**" button
4. Select Uninstall Method
   Select "**Automatic**" and click "**Next**"
5. The uninstall of Ad-Aware SE Professional is completed when the program exits

4 The Ad-Aware Interface

Quick launch menu

Ad-Watch
Starts the Ad-Watch real-time monitor

Settings
Opens the settings where the settings can be changed

Quarantine
Open the Quarantine Manager where the quarantine files can be viewed and managed

WebUpdate
Start the WebUpdate where you can check for updated definition files

Information
Information about Ad-Aware SE

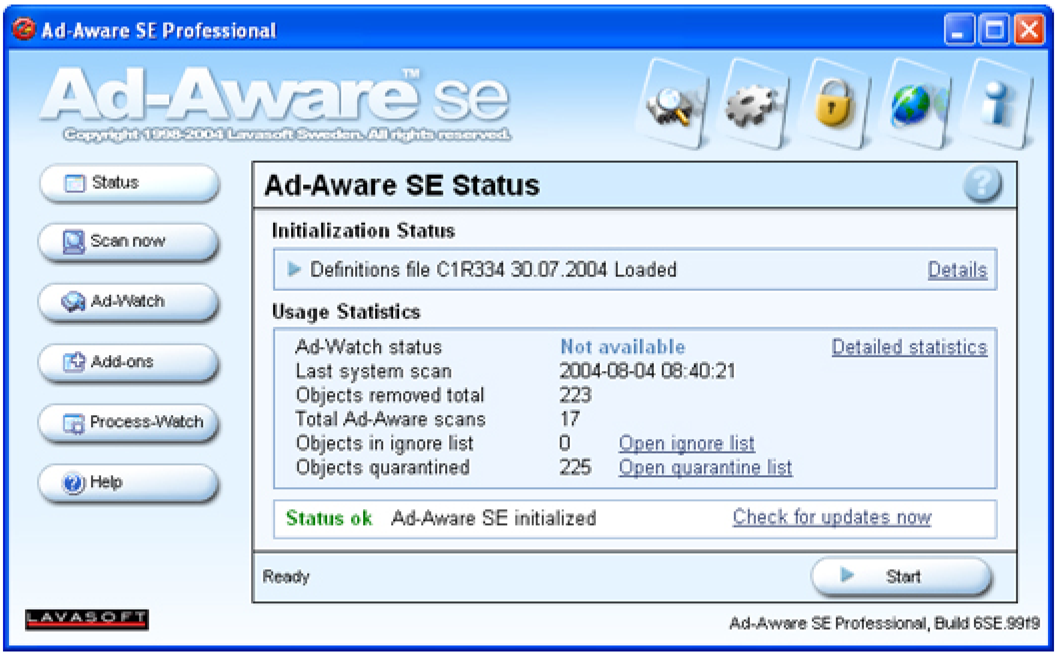
Main menu buttons

Status	Opens the Ad-Aware Main Status screen
Scan now	Opens the Preparing System Scan screen
Ad-Watch	Starts the Ad-Watch real-time monitor
Add-ons	Opens the Add-ons screen
Process-Watch	Opens the process browser Process-Watch
Help	Opens the Help file

Quick Tip button

? Shows the quick help tips for the current screen

4.1 Main Status screen



Ad-Aware SE Status

Initialization Status

Definitions file C1R334 30.07.2004 Loaded Details

Usage Statistics

Ad-Watch status	Not available	Detailed statistics
Last system scan	2004-08-04 08:40:21	
Objects removed total	223	
Total Ad-Aware scans	17	
Objects in ignore list	0	Open ignore list
Objects quarantined	225	Open quarantine list

Status ok Ad-Aware SE initialized Check for updates now

Ready Start

Ad-Aware SE Professional, Build 6SE.99f9

Initialization Status

Shows the current definition file loaded in Ad-Aware SE
Details: Shows the details of the current definition file that is loaded

Usage Statistics

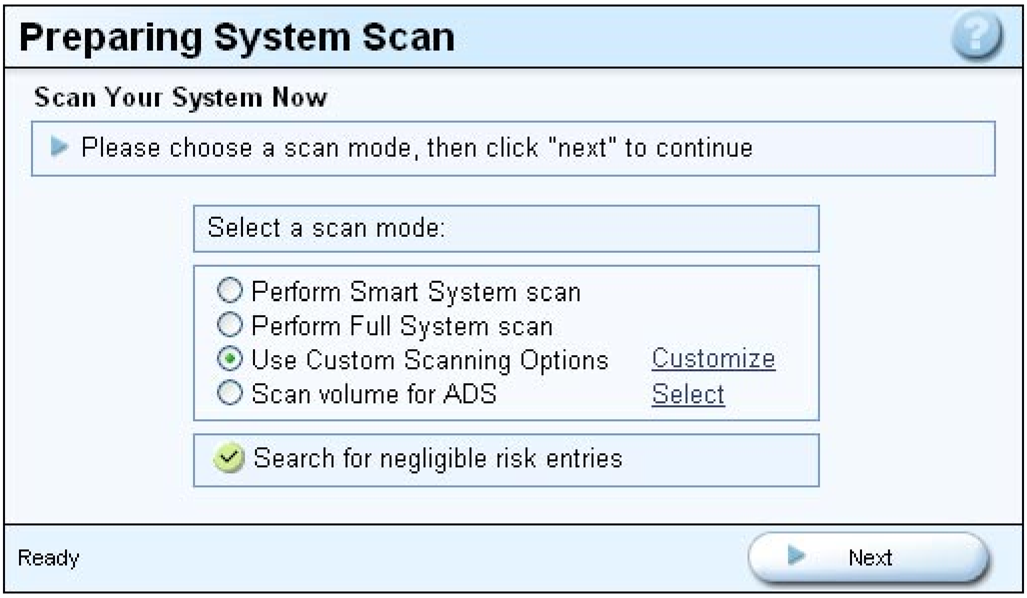
Ad-Watch status: Shows if Ad-Watch is loaded or not
Detailed Statistics: Takes you to the Statistics screen
Last system scan: Shows the date and time of the last scan
Objects removed total: Shows the total number of objects that have been removed since installation or the statistics have been reset
Total Ad-Aware scans: Shows the total number of scans that have been preformed since installation or the statistics have been reset
Objects in ignore list: Shows the total number of objects that are currently being ignored
Open ignore list: Takes you to the Ignore List manager where the ignored objects can be viewed, restored, or removed from the ignore list
Objects quarantined: Shows the total number of objects that are currently in quarantine
Open quarantine list: Takes you to the Quarantine Manager where the objects in quarantine can be viewed and/or restored. You can also delete old quarantines at your discretion

Status

Status ok Ad-Aware SE initialized: Ad-Aware has been initialized without problems
Warning! Definition file not found or corrupted!: The definition file could not be loaded. Run WebUpdate to download the latest definition file.
Check for updates now: Opens WebUpdate
Start: Takes you to the Preparing System Scan screen

4.2 Preparing System Scan

Important Note! Before performing a scan, be sure that you have the most recent definitions file by using WebUpdate. This can be done manually from the main status screen. See the Getting Started or Update the definition file chapters pages for instructions.



Preparing System Scan

Scan Your System Now

Please choose a scan mode, then click "next" to continue

Select a scan mode:

- ○ Perform Smart System scan
- ○ Perform Full System scan
- ● Use Custom Scanning Options Customize
- ○ Scan volume for ADS Select

✓ Search for negligible risk entries

Ready

Select scan mode

Perform smart system scan

The smart system scan is a fast system check and should be used only for daily system maintenance; i.e. you are sure that your system is clean and have performed a full system scan or an in-depth custom scan on your main hard drive at least once during the month. If this is your first scan, you suspect that your system has become infected with suspicious content, or you have used another antispyware product prior to installing and/or using Ad-Aware SE, please be sure to perform a full system scan (see below).

In most cases a Smart Scan will detect all content present on your system as Ad-Aware SE is capable of determining if further scanning is required. This does not include archived content however so a first time full system scan is highly recommended and at regular intervals to ensure that your system is clean.

When performing a smart scan the following scan settings are used:

- Full Memory Scan is performed
- Registry Scan is performed
- Deep Registry scan is performed
- Cookie-Scan is performed
- Favorites are scanned
- Hosts file is scanned
- Conditional scans are performed

Note! Smart scan does not scan within archives.

Perform full system scan

This is the in-depth scan mode that scans your whole computer for Spyware infections. The full system scan is highly recommended for the first time you use Ad-Aware SE, if you have reason to believe your computer is infected with Spyware which isn't found using the smart scan, or you have used another antispyware product prior to installing and/or using Ad-Aware SE. The full system scan is notably slower than the smart system scan, but has a higher probability to detect Spyware infections in archives or has been installed on drives other than your main hard disk.

The full system scan uses the same scan settings as the smart system scan, but also scans all fixed drives and archive files.

Use custom scanning options

You can customize Ad-Aware SE to scan on specific folders or drives. This option allows you to select or deselect drives and folders

Customize: Takes you to the Scan Settings screen. On this screen open the drive and folder selection screen by clicking on the "**Select drives & folders to scan**"

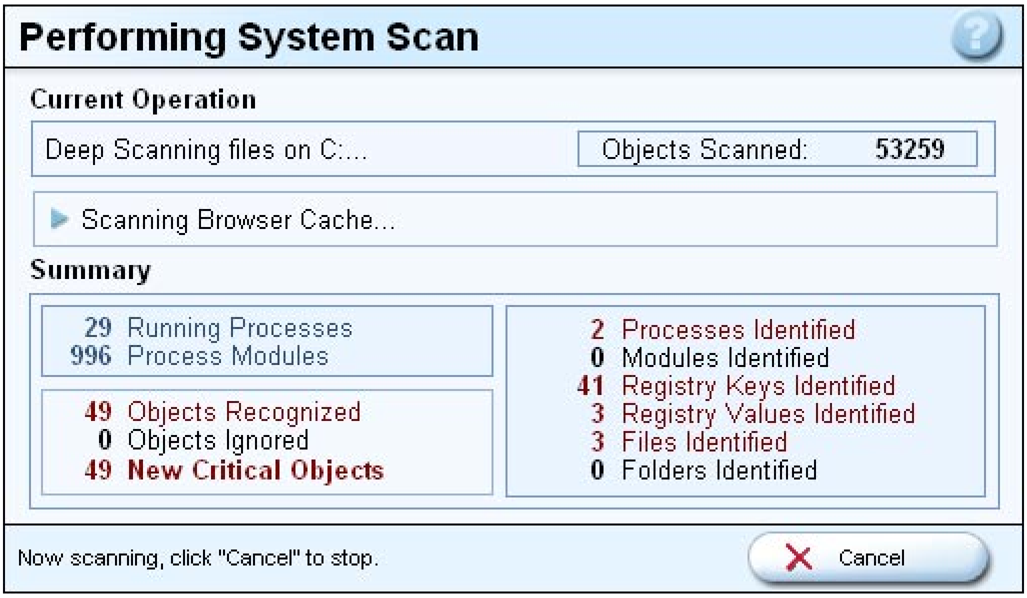
Scan ADS on drives\folders
The ADS (Alternate Data Streams) scan is performed in two steps. In the first phase, a regular disk scan is performed during which information is accumulated and cached. Any file scanned during this phase is being counted as a separately scanned object.

During the second phase detected streams are examined and, if appropriate, scanned. Every stream is counted as a separately scanned object during this phase. This design makes sure that the ADS scan does not bypass critical objects, just because they have none or are not attached to a DataStream.

Select: The ADS scan requires that the user manually selects one or more folders and/or drives to be scanned.

Search for negligible risk entries
Negligible risk entries are not considered to be a threat. They consist of MRU (Most Recently Used items) lists which store information about the most recently used items, for example files, search words and programs. The MRU lists can be removed if the user desires.

4.3 Performing System Scan



Performing System Scan

Current Operation

Deep Scanning files on C:... Objects Scanned: 53259

Scanning Browser Cache...

Summary

29 Running Processes
996 Process Modules

49 Objects Recognized
0 Objects Ignored
49 New Critical Objects

2 Processes Identified
0 Modules Identified
41 Registry Keys Identified
3 Registry Values Identified
3 Files Identified
0 Folders Identified

Now scanning, click "Cancel" to stop.

Current Operation
Shows what operation Ad-Aware is currently performing
Objects Scanned: Shows how many objects that have been scanned so far

Summary
The statistics in this section are updated continuously during the scan.

Running Processes: Shows the total number of processes running on your system during the scan and can include detected as well as normal system processes. See the results at the end of your scan or the log file for those that have been identified with privacy implications.
Process Modules: Shows the number of scanned process modules. As above these are associated with the running processes and represent a total number. See the results at the end of your scan or the log file for those that have been identified with privacy implications.

Objects Recognized: The total number of recognized objects during the scan
Objects Ignored: The number of objects that have been ignored during the scan
New Critical Objects: The number of new critical objects that have been detected

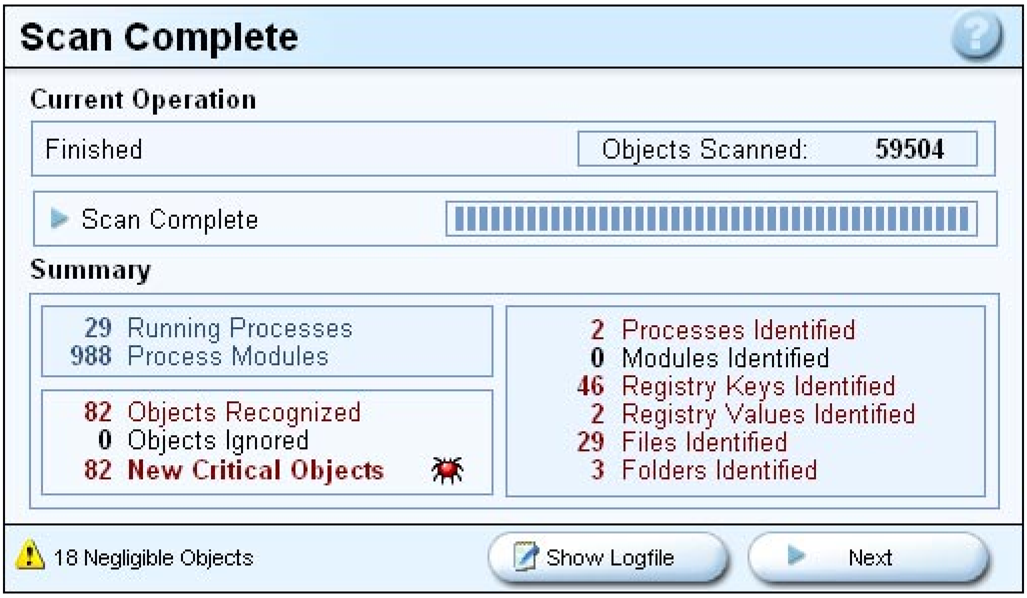
Processes Identified: The total number of detected processes. This only lists the number of processes that are targeted or suspicious.
Modules Identified: The total number of detected process modules
Registry Keys Identified: The total number of detected targeted or suspicious registry keys
Registry Values Identified: The total number of detected suspicious registry values
Files Identified: The total number of detected suspicious files
Folders Identified: The total number of detected suspicious folders

Button

Cancel: Stops the scan

4.4 Scan Complete

When a scan is completed the Performing System Scan screen will change name to "**Scan Complete**".



Scan Complete

Current Operation

Finished
Objects Scanned: 59504

Scan Complete

Summary

29 Running Processes
988 Process Modules

82 Objects Recognized
0 Objects Ignored
82 New Critical Objects

2 Processes Identified
0 Modules Identified
46 Registry Keys Identified
2 Registry Values Identified
29 Files Identified
3 Folders Identified

18 Negligible Objects

Current Operation

Shows that the scan has been completed
Objects Scanned: Shows the total number of objects that have been scanned

Summary

Running Processes: Shows the total number of processes running on your system during the scan and can include detected as well as normal system processes. See the results at the end of your scan or the log file for those that have been identified with privacy implications.
Process Modules: Shows the number of scanned process modules. As above these are associated with the running processes and represent a total number. See the results at the end of your scan or the log file for those that have been identified with privacy implications.

Objects Recognized: The total number of recognized objects during the scan
Objects Ignored: The number of objects that have been ignored during the scan
New Critical Objects: The number of new critical objects that have been detected

Processes Identified: The total number of detected processes. This only lists the number of

processes that are targeted or suspicious.
Modules Identified: The total number of detected process modules
Registry Keys Identified: The total number of detected targeted or suspicious registry keys
Registry Values Identified: The total number of detected suspicious registry values
Files Identified: The total number of detected suspicious files
Folders Identified: The total number of detected suspicious folders

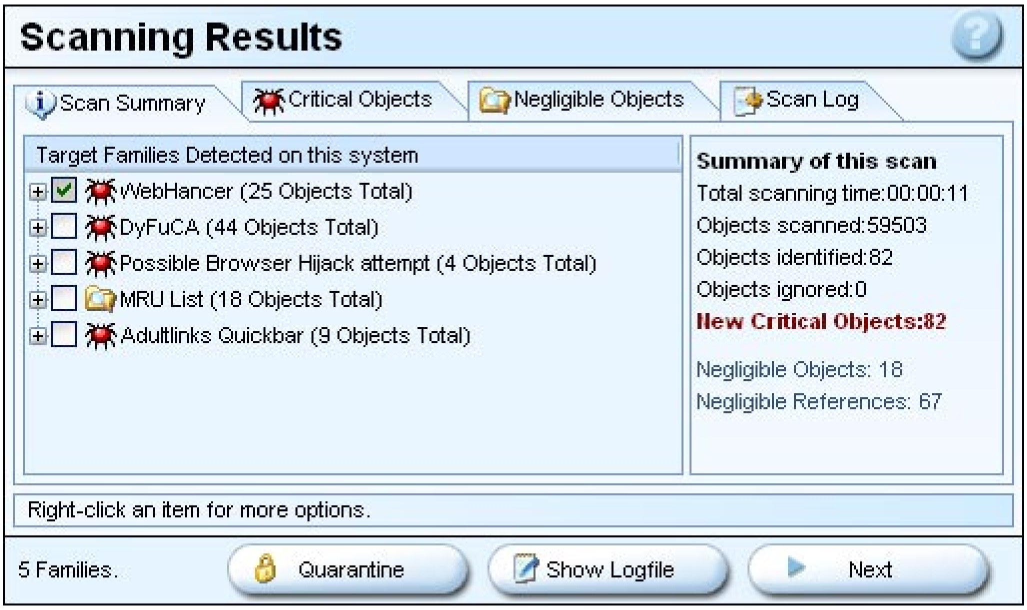
Negligible Objects: The number of negligible objects detected. These objects are not considered to be a threat. They consist of MRU (Most Recently Used items) lists and can be removed if the user desires.

Buttons
Show Logfile: Takes you to the scan log screen
Next: Takes you to the Scanning Results screens where more information about the objects detected during the scan is available

4.5 Scanning Results

4.5.1 Scan Summary

Shows a summary of the Scanning Results.



Target Families Detected on this system

☑ WebHancer (25 Objects Total)
□ DyFuCA (44 Objects Total)
□ Possible Browser Hijack attempt (4 Objects Total)
□ MRU List (18 Objects Total)
□ Adultlinks Quickbar (9 Objects Total)

Summary of this scan
Total scanning time:00:00:11
Objects scanned:59503
Objects identified:82
Objects ignored:0
New Critical Objects:82

Negligible Objects: 18
Negligible References: 67

Right-click an item for more options.

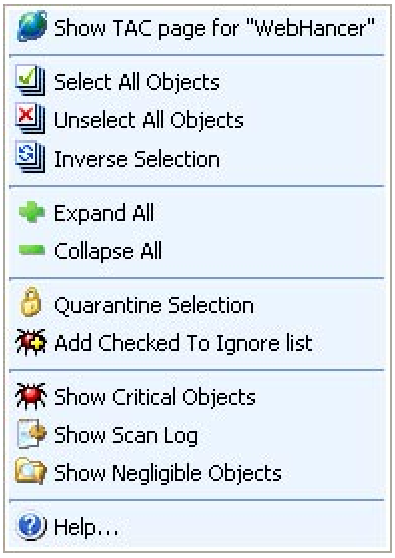
5 Families.

Target families detected on this system: Sorts and lists the objects detected by target family. Clicking the [+] will show the TAC rating. Checking the box will mark all objects in the group for removal. This will be carried over into the Critical and Negligible Objects tabs as well; unchecking them will have the reverse action.

Summary of this scan: Shows the summary of the scan results in aggregate as well as display the total scan time. This information is also appended to the end of the log file.

Buttons
Quarantine: Puts the selected objects in a quarantine file. This can be useful when you don't want to quarantine all objects detected during a scan, as the automatic quarantine option does or to quarantine by family, vendor, or type of detected content. **Note!** You will be prompted to add a filename.
Show Logfile: Displays the log file created during the scan
Next: Takes you to the removal confirmation window

Right-click to open the context menu where more options are available



Context menu

Show TAC page for "vendor name": Shows the TAC page for the target family*

Select all objects: Selects all objects found
Deselect all objects: Deselects all objects found
Inverse selection: Inverses the selection

Expand all: This will expand each family to show the TAC rating
Collapse All: This will collapse each family

Quarantine selected: Quarantines all selected objects. **Note!** You will be prompted to add a filename.
Move to ignore list: Adds the selected objects to the Ignore List

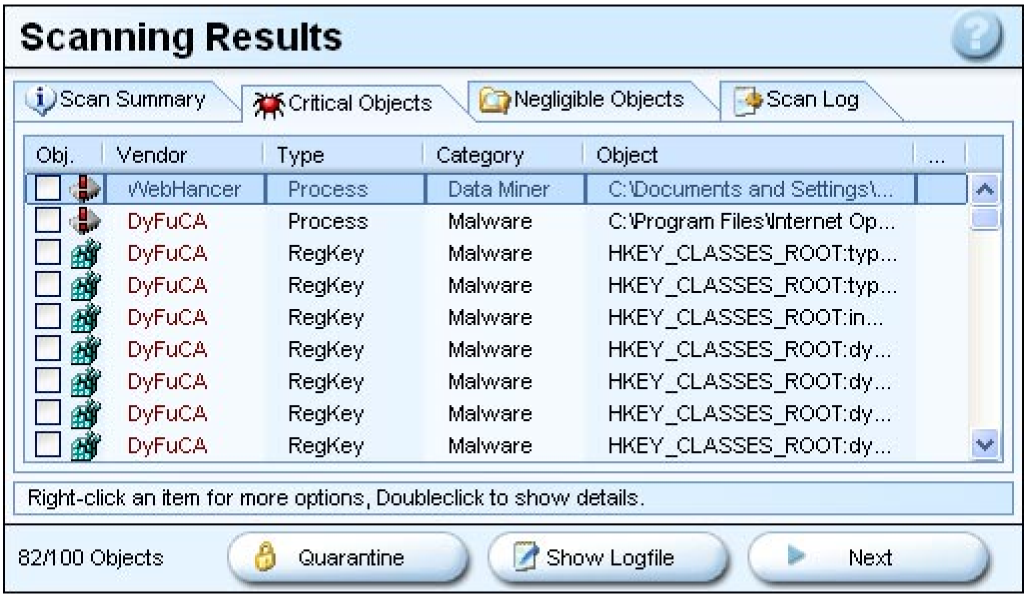
Show Critical Objects: Takes you to the Critical Objects tab
Show Scan Log: Takes you to the Scan Log tab
Show Negligible Objects: Takes you to the Negligible Objects tab

Help: Opens the Help file

* You must be connected to the Internet to access the TAC

4.5.2 Critical Objects

Objects shown here may pose a threat and should be considered for removal.



Obj.	Vendor	Type	Category	Object	...
☐	WebHancer	Process	Data Miner	C:\Documents and Settings\...	
☐	DyFuCA	Process	Malware	C:\Program Files\Internet Op...	
☐	DyFuCA	RegKey	Malware	HKEY_CLASSES_ROOT:typ...	
☐	DyFuCA	RegKey	Malware	HKEY_CLASSES_ROOT:typ...	
☐	DyFuCA	RegKey	Malware	HKEY_CLASSES_ROOT:in...	
☐	DyFuCA	RegKey	Malware	HKEY_CLASSES_ROOT:dy...	
☐	DyFuCA	RegKey	Malware	HKEY_CLASSES_ROOT:dy...	
☐	DyFuCA	RegKey	Malware	HKEY_CLASSES_ROOT:dy...	
☐	DyFuCA	RegKey	Malware	HKEY_CLASSES_ROOT:dy...	

Right-click an item for more options, Doubleclick to show details.

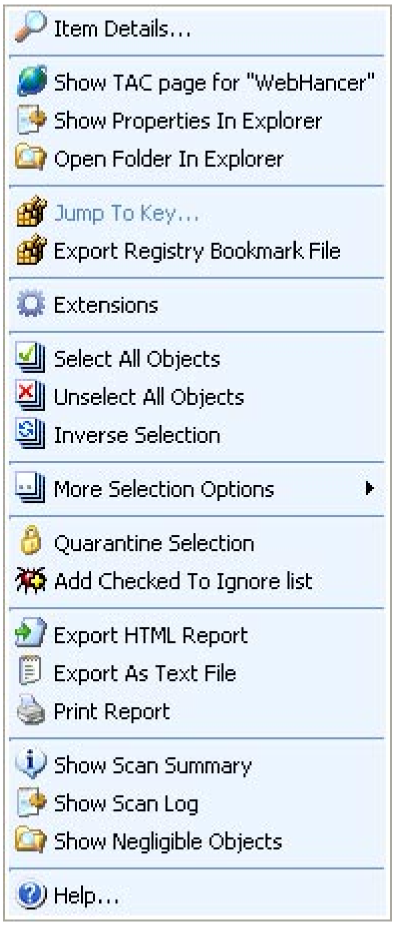
82/100 Objects

Obj.: Select objects by checking the box. This section will also contain easy to identify symbols for the type of object listed
Vendor: Names the company that developed the object or the target family
Type: Tells what kind of object it is, such as File, Folder, Registry Value etc.
Category: Tells the category that Lavasoft has it listed in, such as Data Miner, Malware etc.
Object: Tells where the object is located, its path in Explorer, or its location in the Registry
Comment: includes the name of the object and a brief description; to read the complete text in the comment scroll to the right side of the screen, open the window full screen, hover your mouse over the entry, or use the right click context menu

Buttons

Quarantine: Puts the selected objects in a quarantine file. This can be useful when you don't want to quarantine all objects detected during a scan, as the automatic quarantine option does or to quarantine by family, vendor, or type of detected content. **Note!** You will be prompted to add a filename.
Show Logfile: Displays the log file created during the scan
Next: Takes you to the removal confirmation window

Right-click to open the context menu where more options are available



Context menu

Item Details: Opens the Object Details window that displays the TAC information for the object and a link to the objects TAC webpage.*

Show TAC page for "vendor name": Shows the TAC page for the selected object*
Show properties in Explorer: Shows the properties for the selected object in Windows Explorer
Open folder in Explorer: Opens the folder that contains the object in Windows Explorer

Jump to key: Opens the registry key for the selected object **Note!** This requires RegHance to be installed and linked to in the Ad-Aware SE Default Settings screen.
Export Registry Bookmark File: Exports the registry bookmarks to a .reg file in the folder that you choose

Extensions: The extensions available on your computer are listed here. For more information read the Add-ons chapter

Select all Marked objects: Selects all marked (highlighted) objects in the list
Deselect all Marked objects: Deselects all marked (highlighted) objects
Inverse selection: Inverses the selection

More Selection Objects: Opens a new menu with more select/deselect options
Select all RegValue Objects: Selects all RegValue objects if any are present
Deselect all RegValue Objects: Deselects all RegValue objects if any are present

Select all "vendor name" objects: Selects all objects by the same vendor
Deselect all "vendor name" objects: Deselects all objects by the same vendor

Select all marked objects: Selects all highlighted objects
Deselect all objects: Deselects all highlighted objects

Quarantine selected: Adds all selected objects to an archival quarantine file Note! You will be prompted to enter a filename
Add Checked To Ignore List: Adds all selected objects to the Ignore List.

Export HTML Report: Exports a report in HTML format
Export as Text File: Exports a report in text format
Print Report: Prints the report

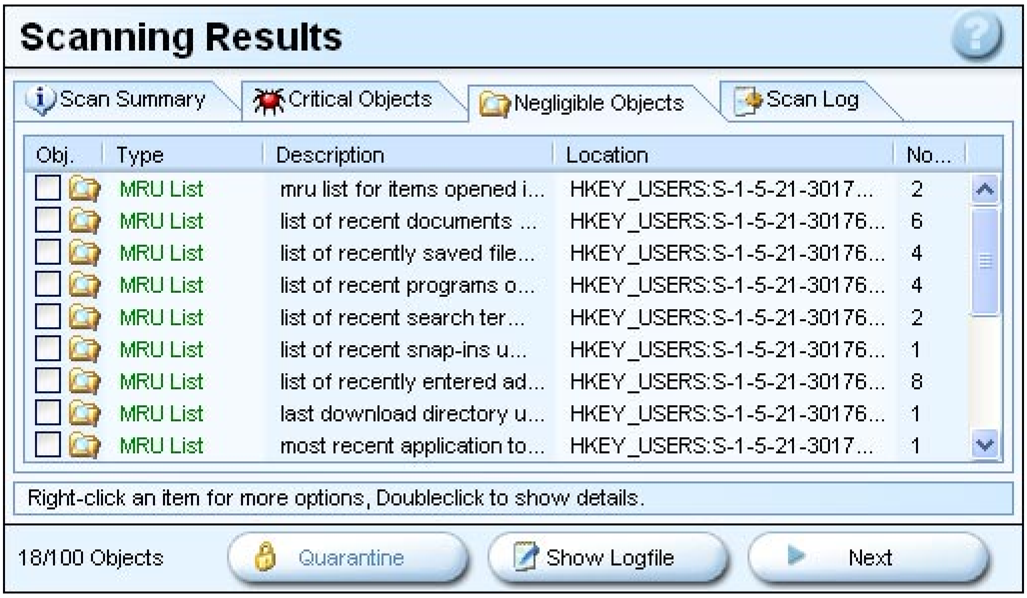
Show Scan Summary: Takes you to the Scan Summary tab
Show Scan Log: Takes you to the Scan Log tab
Show Negligible Objects: Takes you to the Negligible Objects tab

Help: Opens the Help file

* You must be connected to the Internet to access the TAC

4.5.3 Negligible Objects

Objects shown here are not considered to be a threat. They consist of MRU (Most Recently Used items) lists. These can be removed if the user desires.



Obj.	Type	Description	Location	No...
□	MRU List	mru list for items opened i...	HKEY_USERS:S-1-5-21-3017...	2
□	MRU List	list of recent documents ...	HKEY_USERS:S-1-5-21-30176...	6
□	MRU List	list of recently saved file...	HKEY_USERS:S-1-5-21-30176...	4
□	MRU List	list of recent programs o...	HKEY_USERS:S-1-5-21-30176...	4
□	MRU List	list of recent search ter...	HKEY_USERS:S-1-5-21-30176...	2
□	MRU List	list of recent snap-ins u...	HKEY_USERS:S-1-5-21-30176...	1
□	MRU List	list of recently entered ad...	HKEY_USERS:S-1-5-21-30176...	8
□	MRU List	last download directory u...	HKEY_USERS:S-1-5-21-30176...	1
□	MRU List	most recent application to...	HKEY_USERS:S-1-5-21-3017...	1

Right-click an item for more options, Doubleclick to show details.

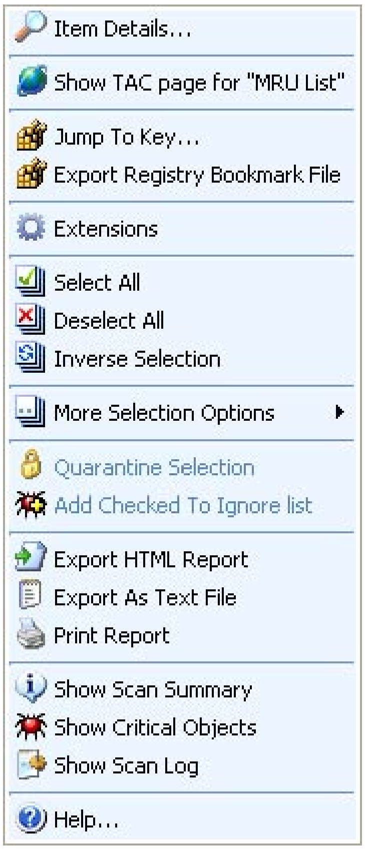
18/100 Objects

Obj.: Select objects by checking the box
Type: Tells the type of the object
Description: A brief description of the object
Location: Tells the location of the object
No. Items: Tells the number of objects in each MRU List

Buttons

Quarantine: Puts the selected objects in a quarantine file. This can be useful when you don't want to quarantine all objects detected during a scan, as the automatic quarantine option does or to quarantine by family, vendor, or type of detected content. **Note!** You will be prompted to add a filename.
Show Logfile: Displays the log file created during the scan
Next: Takes you to the removal confirmation window

Right-click to open the context menu where more options are available



Context menu

Item Details: Opens the Object Details window that displays the TAC information for the object and a link to the objects TAC webpage.*

Show TAC page for "vendor name": Shows the TAC page for the selected object*
Show properties in Explorer: Shows the properties for the selected object in Windows Explorer
Open folder in Explorer: Opens the folder that contains the object in Windows Explorer

Jump to key: Opens the registry key for the selected object **Note!** This requires RegHance to be installed and linked to in the Ad-Aware SE Default Settings screen.
Export Registry Bookmark File: Exports the registry bookmarks to a .reg file in the folder that you choose

Extensions: The extensions available on your computer are listed here. For more information read the Add-ons chapter

Select all Marked objects: Selects all marked (highlighted) objects in the list
Deselect all Marked objects: Deselects all marked (highlighted) objects
Inverse selection: Inverses the selection

More Selection Objects: Opens a new menu with more select/deselect options
Select all marked objects: Selects all highlighted objects
Deselect all objects: Deselects all highlighted objects

Quarantine selected: Adds all selected objects to an archival quarantine file **Note!** You will be prompted to enter a filename
Add Checked To Ignore List: Adds all selected objects to the Ignore List.

Export HTML Report: Exports a report in HTML format
Export as Text File: Exports a report in text format
Print Report: Prints the report

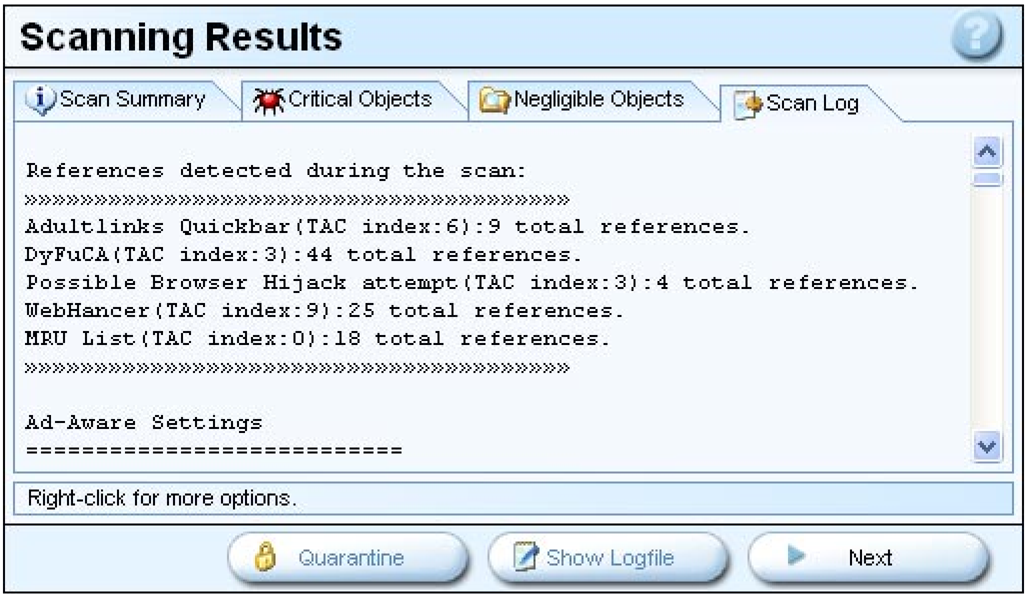
Show Scan Summary: Takes you to the Scan Summary tab
Show Scan Log: Takes you to the Scan Log tab
Show Negligible Objects: Takes you to the Negligible Objects tab

Help: Opens the Help file

* You must be connected to the Internet to access the TAC

4.5.4 Scan Log

Shows the log file created during the scan. The log file contains information about the scan, for example which settings were used, objects detected and processes that were running on the computer during the scan. You can adjust the amount and type of information in the configurations menus

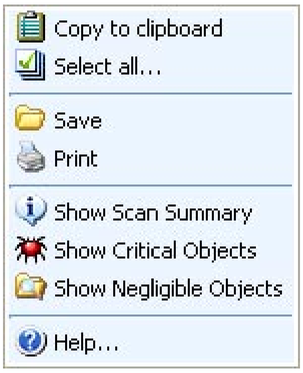


```
References detected during the scan:
»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»
Adultlinks Quickbar(TAC index:6):9 total references.
DyFuCA(TAC index:3):44 total references.
Possible Browser Hijack attempt(TAC index:3):4 total references.
WebHancer(TAC index:9):25 total references.
MRU List(TAC index:0):18 total references.
»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»

Ad-Aware Settings
===========================
```

Right-click for more options.

Right-click to open the context menu where more options are available



Buttons

Quarantine: Puts the selected objects in a quarantine file. This can be useful when you don't want to quarantine all objects detected during a scan, as the automatic quarantine option does or to quarantine by family, vendor, or type of detected content. **Note!** You will be prompted to add a filename.

Show Logfile: Displays the log file created during the scan
Next: Takes you to the removal confirmation window

Context menu

Copy to Clipboard: Copies the selected text to the clipboard
Select all: Selects the text in the log file. **Tip!** You can use the keyboard shortcut **Ctrl + C** to copy the text after highlighting the text you wish to copy

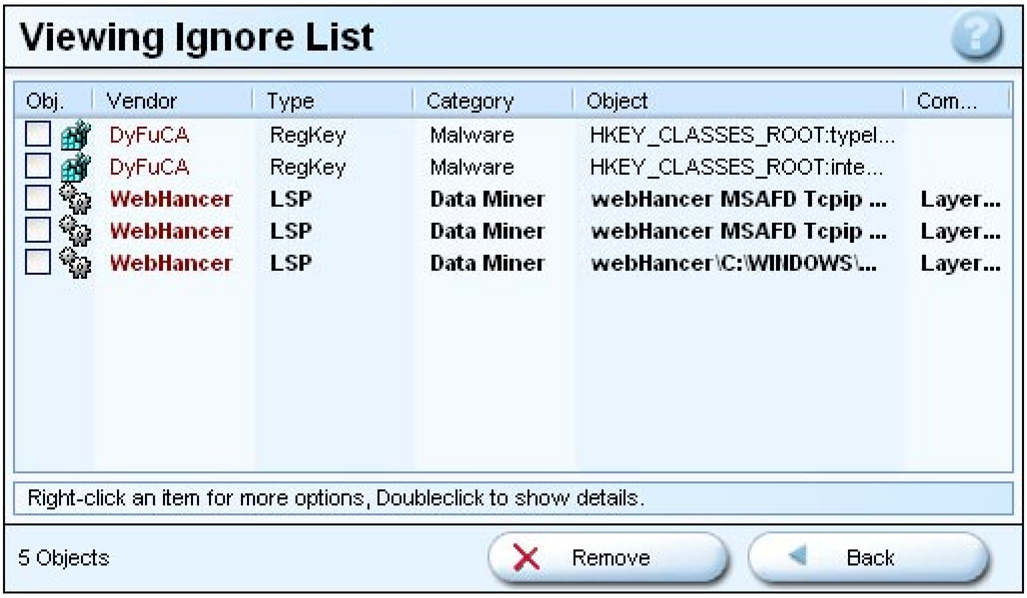
Save: Save the log file to the chosen location
Print: Prints the log file

Show Scan Summary: Takes you to the Scan Summary tab
Show Critical Objects: Takes you to the Critical Objects tab
Show Negligible Objects: Takes you to the Negligible Objects tab

Help: Opens the Help file

4.6 Ignore list

Lists all objects that have been added to the ignore list



Viewing Ignore List

Obj.	Vendor	Type	Category	Object	Com...
☐	DyFuCA	RegKey	Malware	HKEY_CLASSES_ROOT:typel...	
☐	DyFuCA	RegKey	Malware	HKEY_CLASSES_ROOT:inte...	
☐	WebHancer	LSP	Data Miner	webHancer MSAFD Tcpip ...	Layer...
☐	WebHancer	LSP	Data Miner	webHancer MSAFD Tcpip ...	Layer...
☐	WebHancer	LSP	Data Miner	webHancer\C:\WINDOWS\...	Layer...

Right-click an item for more options, Doubleclick to show details.

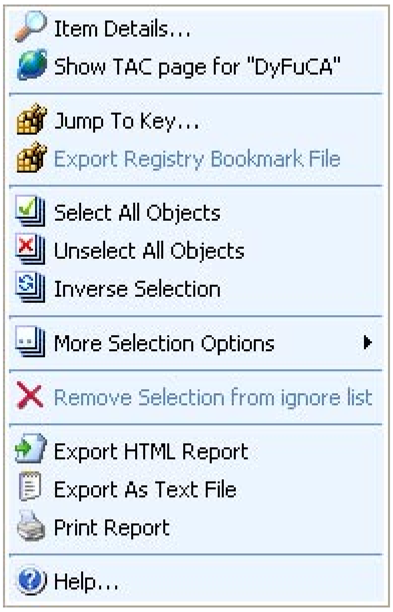
5 Objects

Obj.: Select objects by checking the box
Vendor: Names the company that developed the object or the target family
Type: Tells what kind of object it is, such as File, Folder, Registry Value etc.
Category: Tells the category that Lavasoft has it listed in, such as Data Miner, Malware etc.
Object: Tells where the object is located, its path in Explorer, or its location in the Registry
Comment: The name of the object and a brief comment.

Buttons

Remove: Removes the selected object from the ignore list (i.e. object will be detected in future scans)
Back: Takes you back to the Status screen

Right-click to open the context menu where more options are available



Context menu

Item Details: Opens the Object Details window that displays the TAC information for the object and a link to the objects TAC webpage.*
Show TAC page for "vendor name": Shows the TAC page for the selected object*

Jump to key: Opens the registry key for the selected object **Note!** This requires RegHance to be installed and linked to in the Ad-Aware SE Default Settings screen.
Export Registry Bookmark File: Exports the registry bookmarks to a .reg file in the folder that you choose

Select all Marked objects: Selects all marked (highlighted) objects in the list
Deselect all Marked objects: Deselects all marked (highlighted) objects
Inverse selection: Inverses the selection

More Selection Objects: Opens a new menu with more select/deselect options
Select all RegValue Objects: Selects all RegValue objects if any are present
Deselect all RegValue Objects: Deselects all RegValue objects if any are present

Select all "vendor name" objects: Selects all objects by the same vendor
Deselect all "vendor name" objects: Deselects all objects by the same vendor

Select all marked objects: Selects all highlighted objects
Deselect all objects: Deselects all highlighted objects

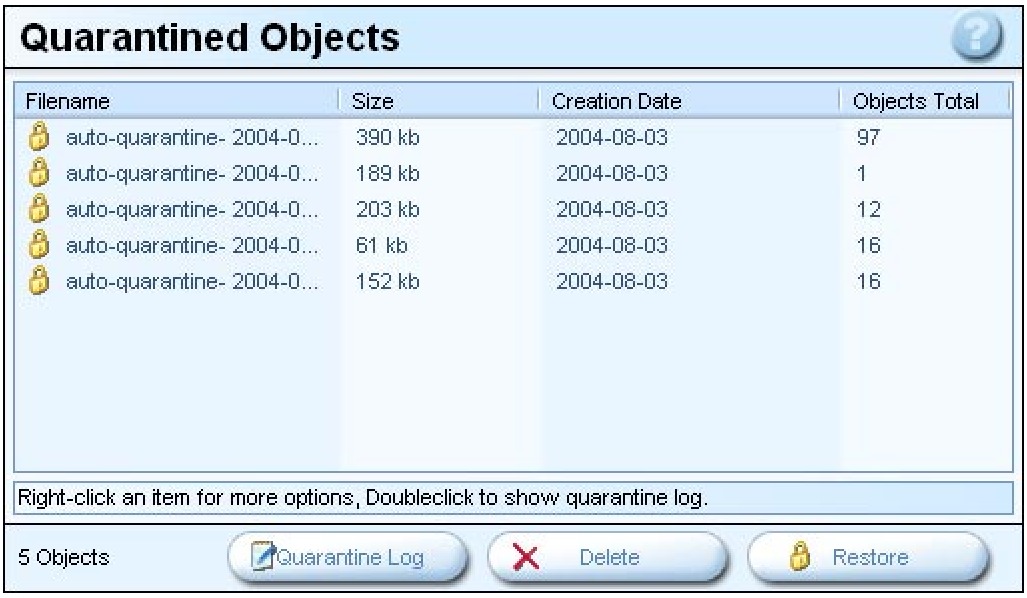
Remove Selection from ignore list: Removes the selected object from the ignore list (i.e. object will be detected in future scans)
Export HTML Report: Exports a report in HTML format
Export as Text File: Exports a report in text format
Print Report: Prints out the report

Help: Opens the Help file

* You must be connected to the Internet to access the TAC

4.7 Quarantined Objects

Lists all the quarantine files that contain content that was previously removed

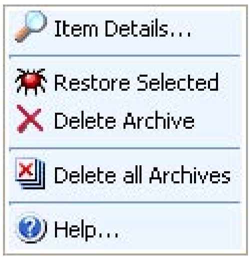


Filename	Size	Creation Date	Objects Total
auto-quarantine- 2004-0...	390 kb	2004-08-03	97
auto-quarantine- 2004-0...	189 kb	2004-08-03	1
auto-quarantine- 2004-0...	203 kb	2004-08-03	12
auto-quarantine- 2004-0...	61 kb	2004-08-03	16
auto-quarantine- 2004-0...	152 kb	2004-08-03	16

Right-click an item for more options, Doubleclick to show quarantine log.

File Name: Shows the file name of the quarantine file
Size: Shows the size of the quarantine file in Kilobytes (KB)
Creation Date: Shows the date the quarantine file was created
Objects Total: Shows the total number of objects included in the selected quarantine file

Right-click to open the context menu where more options are available



Buttons

Quarantine Log: Opens the quarantine log file for the selected archive
Delete: Removes the selected quarantine file
Restore: Restores the objects in the selected quarantine file

Context menu

Item Details: Opens the quarantine log

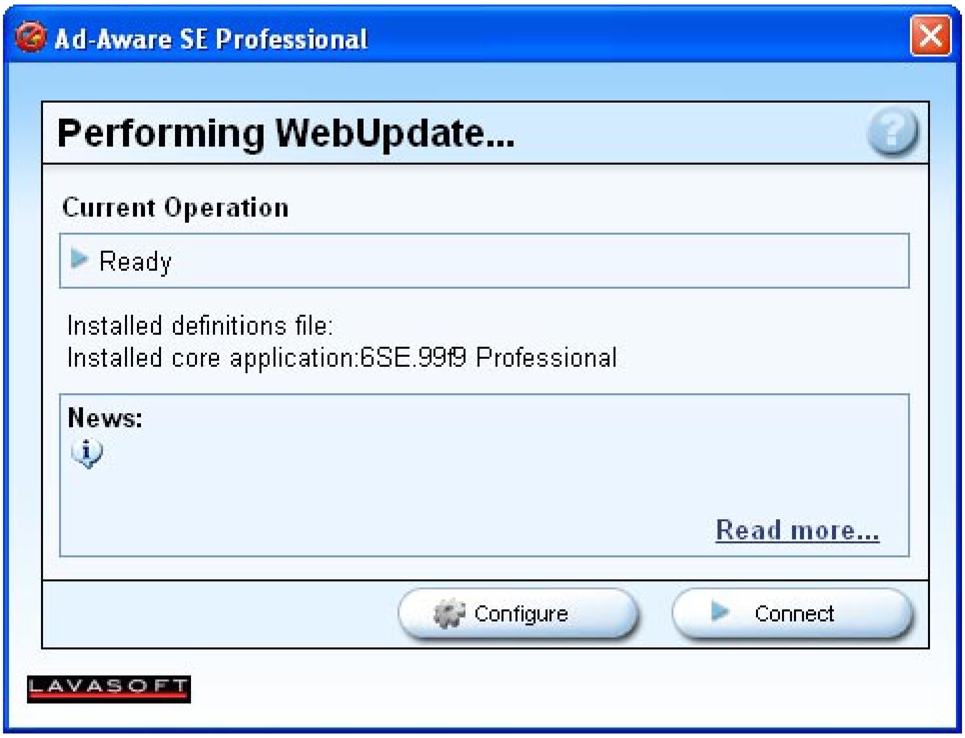
Restore Selected: Reinstalls the objects in the quarantine file
Delete Archive: Deletes the selected quarantine file

Delete all Archives: Deletes ALL quarantine files

Help: Opens the Help file

4.8 WebUpdate

4.8.1 Performing WebUpdate... main screen



Ad-Aware SE Professional

Performing WebUpdate...

Current Operation

Ready

Installed definitions file:
Installed core application:6SE.99f9 Professional

News:

Current Operation: Shows the current operation that is being performed by WebUpdate. When first opened, the message will be "**Ready**" to indicate that WebUpdate is initialized and ready to be used
Progress bar: Shows the progress of the definitions file download

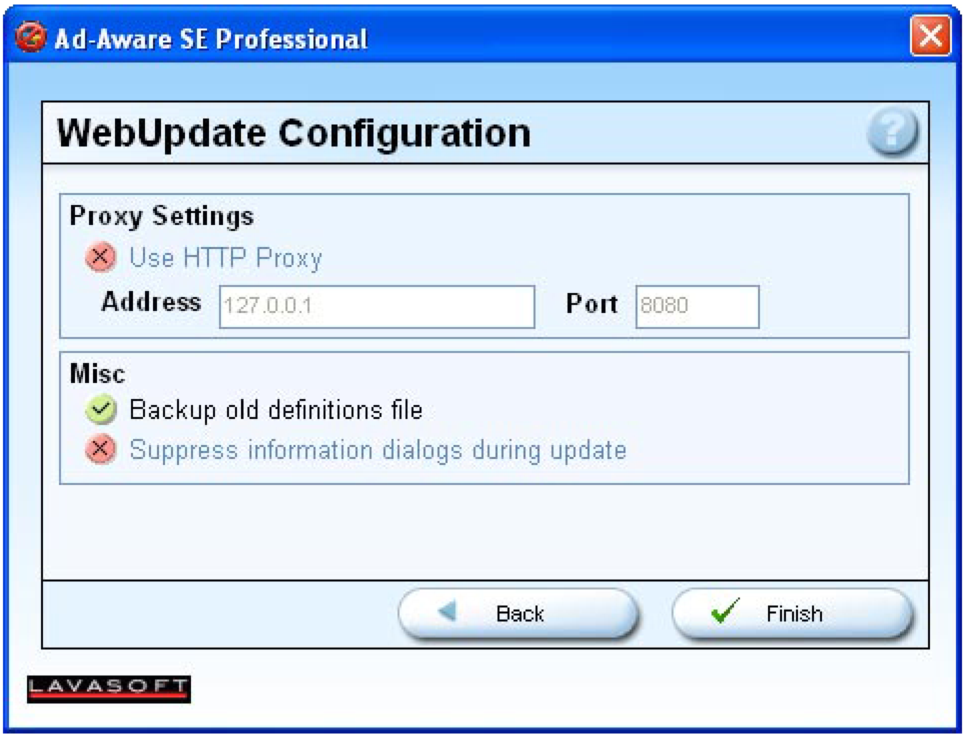
Installed definition file: Shows the version of the currently loaded definition file.
Installed Core Application: Shows the version and build of Ad-Aware SE that is installed

News: A summary of the latest news from Lavasoft. No content will be displayed here until WebUpdate has connected to the Lavasoft servers. If information is displayed, you can click the "**Read more…**" link that will take you to the detailed news article related to the news summary

Buttons

Configure: Opens the WebUpdate Configuration window
Connect: Connects to the server, downloads and installs the latest definition file if one is available

4.8.2 WebUpdate Configuration screen



Ad-Aware SE Professional

WebUpdate Configuration

Proxy Settings

☒ Use HTTP Proxy

Address 127.0.0.1 Port 8080

Misc

✓ Backup old definitions file

☒ Suppress information dialogs during update

Proxy Settings

Use HTTP Proxy: Turns on\off the Proxy Settings.
Address: Enter the IP address that your Proxy uses.
Port: Enter the port that your Proxy uses.

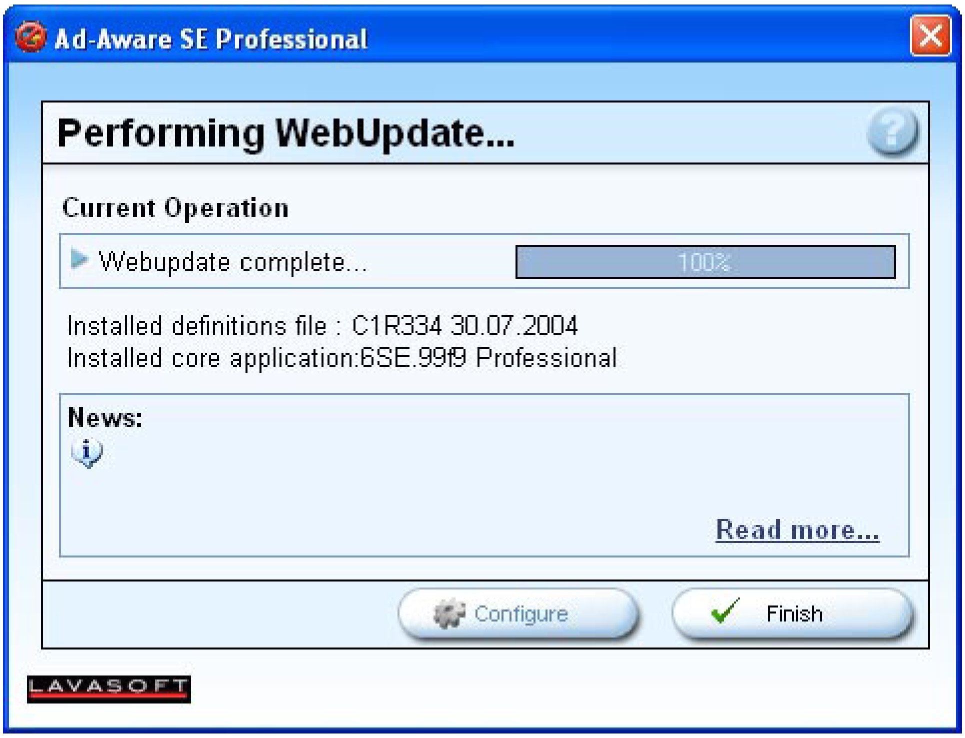
Misc

Backup old definition file: Creates a backup of the current definition file before installing a new one
Suppress information dialogs during update: No notification message will be displayed asking for download confirmation or confirming that the download has finished

Buttons

Back: Returns to the Performing WebUpdate screen
Connect: Connects to the server, downloads and installs the latest definition file if one is available

4.8.3 WebUpdate process completed



Installed definitions file : C1R334 30.07.2004
Installed core application:6SE.99f9 Professional

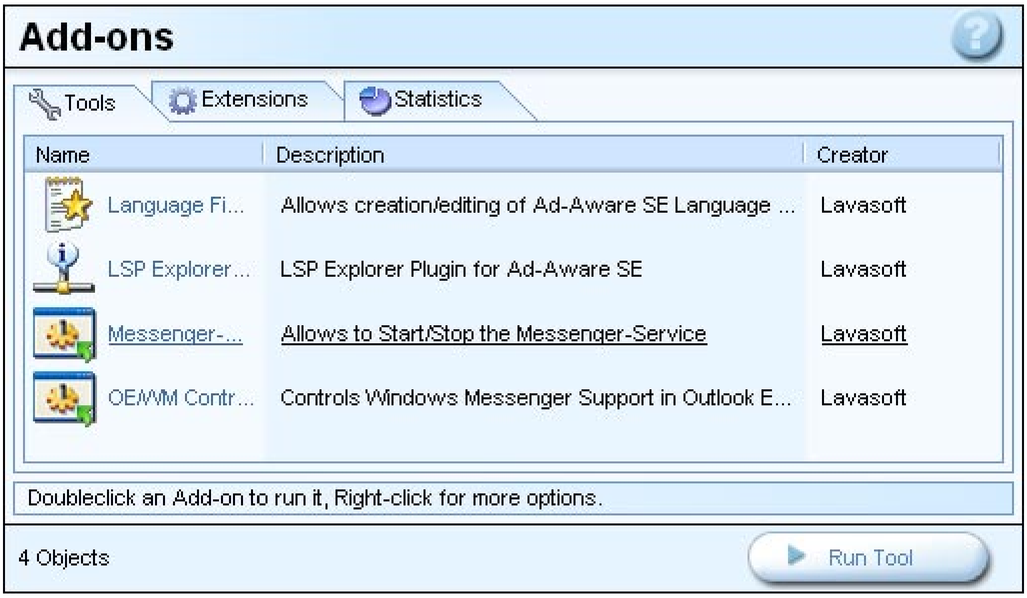
Buttons
Configure: Opens the WebUpdate Configuration window
Finish: Closes WebUpdate and returns you to the Ad-Aware SE Main Status screen

4.9 Add-ons

Tools are stand-alone programs that can be used without performing a scan
Extensions provide information about the objects detected by Ad-Aware SE and offer options for investigating the listed content detected from within the Results screen
Statistics shows information about previous scans

4.9.1 Tools

Lists all tool add-ons installed.



Name	Description	Creator
Language Fi...	Allows creation/editing of Ad-Aware SE Language ...	Lavasoft
LSP Explorer...	LSP Explorer Plugin for Ad-Aware SE	Lavasoft
Messenger-...	Allows to Start/Stop the Messenger-Service	Lavasoft
OE/WM Contr...	Controls Windows Messenger Support in Outlook E...	Lavasoft

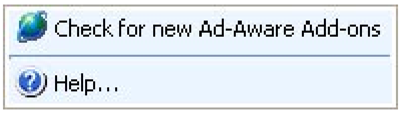
Doubleclick an Add-on to run it, Right-click for more options.

Name: Name of the tool
Description: Short description of the tool
Creator: Shows the name of the company or person that made the tool

Button

Run Tool: Starts the selected tool **Tip!** You can also start a tool by double-clicking on it

Right-click to open the context menu where more options are available



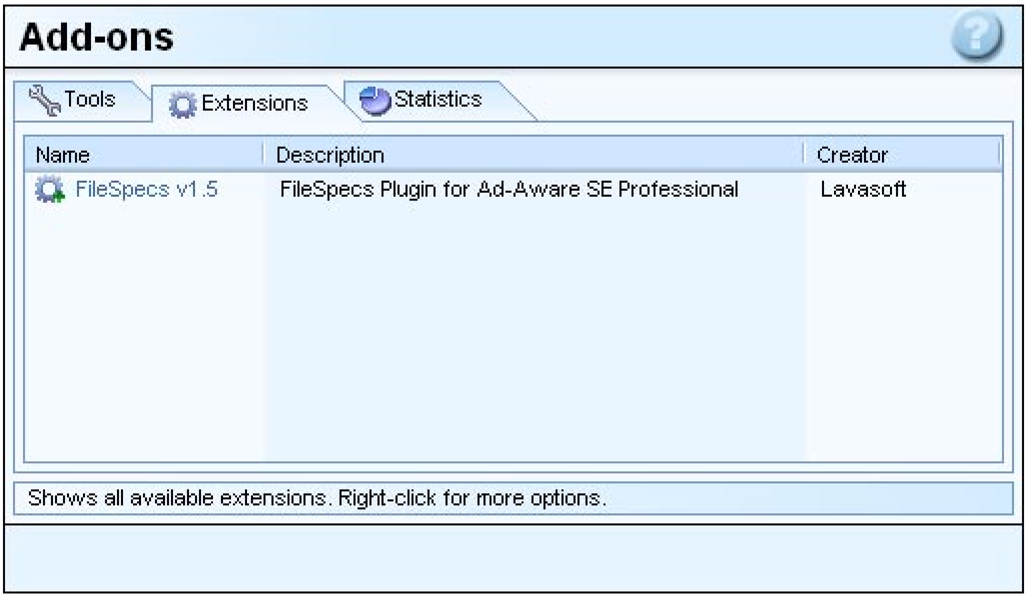
Context menu

Check for new Ad-Aware Add-ons: Takes you to the Lavasoft website where you can find more add-ons*
Help: Opens the Help file

* You must be connected to the Internet to look for add-ons and access the TAC

4.9.2 Extensions

Lists all extensions installed.

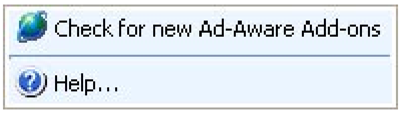


Name	Description	Creator
FileSpecs v1.5	FileSpecs Plugin for Ad-Aware SE Professional	Lavasoft

Shows all available extensions. Right-click for more options.

Name: Name of the tool
Description: Short description of the tool
Creator: Shows the name of the company or person that made the tool

Right-click to open the context menu where more options are available

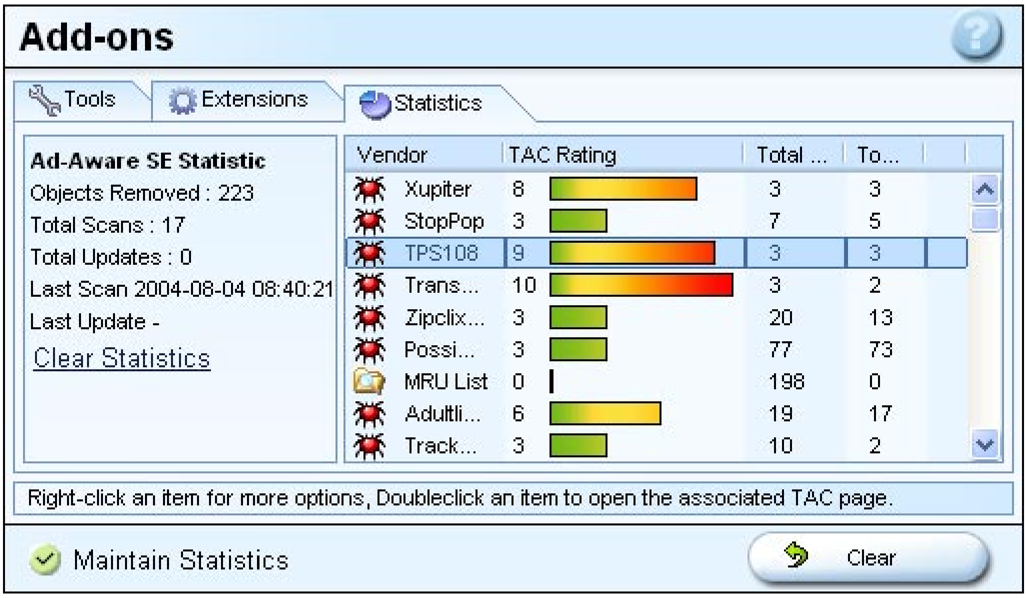


Context menu
Check for new Ad-Aware Add-ons: Takes you to the Lavasoft website where you can find more add-ons*
Help: Opens the Help file

* You must be connected to the Internet to look for add-ons

4.9.3 Statistics

Shows statistics on previous scans



Ad-Aware SE Statistic
Objects Removed : 223
Total Scans : 17
Total Updates : 0
Last Scan 2004-08-04 08:40:21
Last Update -
Clear Statistics

Vendor	TAC Rating	Total ...	To...
Xupiter	8	3	3
StopPop	3	7	5
TPS108	9	3	3
Trans...	10	3	2
Zipclix...	3	20	13
Possi...	3	77	73
MRU List	0	198	0
Adultli...	6	19	17
Track...	3	10	2

Right-click an item for more options, Doubleclick an item to open the associated TAC page.

Vendor: Names the company that developed the object or the target family
TAC Rating: Shows the TAC rating for the target family
Total Found: Shows how many objects of that target family that has been found
Total Removed: Shows how many objects of that target family that has been removed
Last Detected: Shows the date when an object of this target family was last detected

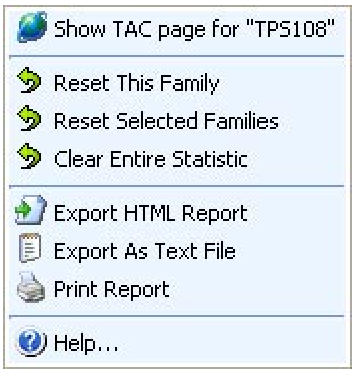
Button

Clear: Clears all statistics

Settings

Maintain Statistics: Ad-Aware keeps statistics of usage if checked

Right-click to open the context menu where more options are available



Context menu

Show TAC page for "vendor name": Shows the TAC page for the target family*

Reset This Family: Resets the statistics for the selected family
Reset Selected Families: Resets the statistics for all selected families
Clear Entire Statistics: Clears all statistics

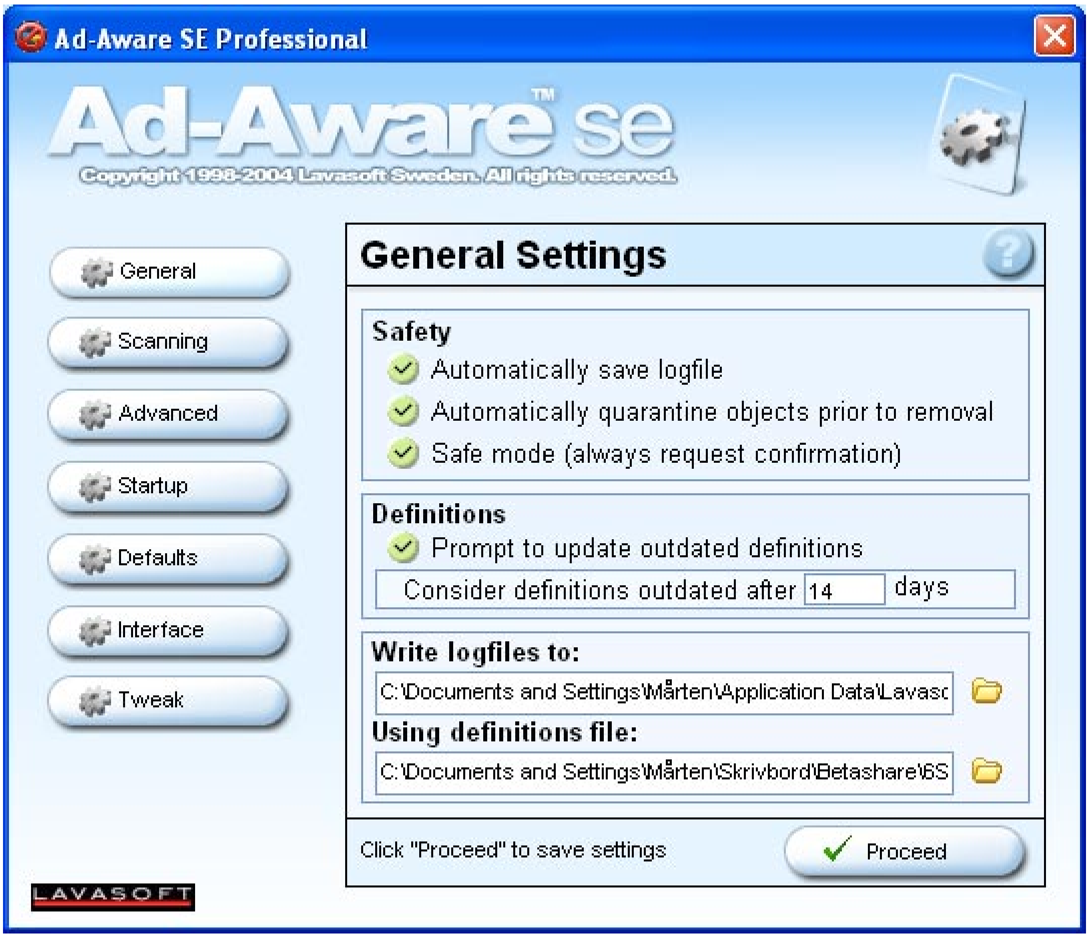
Export HTML Report: Exports a report in HTML format
Export as Text File: Exports a report in text format
Print Report: Prints out the report

Help: Opens the Help file

* You must be connected to the Internet to look for add-ons and access the TAC

4.10 Settings

Settings are used to customize Ad-Aware SE to fit your needs. You can for example change the language or look of the interface, or set up Ad-Aware to update the definition file, scan and remove detected objects automatically on startup.



General Settings

Safety

✓ Automatically save logfile

✓ Automatically quarantine objects prior to removal

✓ Safe mode (always request confirmation)

Definitions

✓ Prompt to update outdated definitions

Consider definitions outdated after 14 days

Write logfiles to:

C:\Documents and Settings\Mårten\Application Data\Lavasc

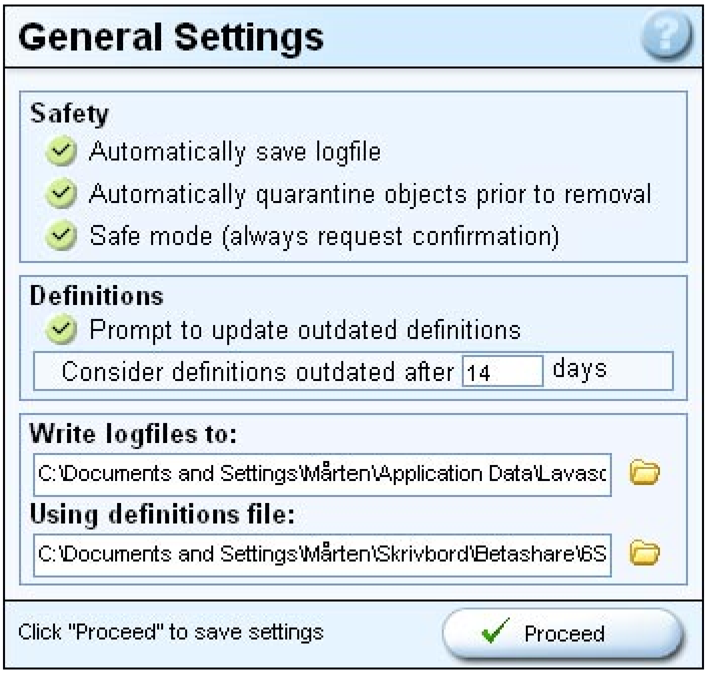
Using definitions file:

C:\Documents and Settings\Mårten\Skrivbord\Betashare\6S

Click "Proceed" to save settings

For a detailed look at each of the separate configurations screens please see the applicable section in this chapter:
General Settings
Scan Settings
Advanced Settings
Startup Settings
Default Settings
Interface Settings
Tweak Settings

4.10.1 General Settings



General Settings

Safety

✓ Automatically save logfile

✓ Automatically quarantine objects prior to removal

✓ Safe mode (always request confirmation)

Definitions

✓ Prompt to update outdated definitions

Consider definitions outdated after 14 days

Write logfiles to:

C:\Documents and Settings\Mårten\Application Data\Lavasc

Using definitions file:

C:\Documents and Settings\Mårten\Skrivbord\Betashare\6S

Click "Proceed" to save settings

Safety Settings

Automatically save log file: A log file will be saved to your computer after each scan.

Automatically quarantine objects prior removal: An automatic quarantine will be created for any items removed when pressing the "**Next**" button on the Scan Results screen

Safe mode (always request confirmation): A dialog box requesting confirmation will be displayed when doing any alterations to objects such as remove or quarantine

Definitions

Prompt to update outdated definition files: Ad-Aware SE will remind you to check for updates when your definition file is outdated*

Consider definitions outdated after "time interval here" days: Sets a time limit that will define when Ad-Aware SE considers the installed definitions file to be outdated. The time interval is pre-set by the user. When activated and when the pre-set time limit has been reached or exceeded, Ad-Aware will present a popup warning when initialized.

***Note to System Administrators!** Turn this feature off if using Ad-Aware SE where end user interaction is not required.

Write logfiles to: Use the browse feature to locate the folder you wish to store the log files in. Click on the folder and navigate to your chosen location

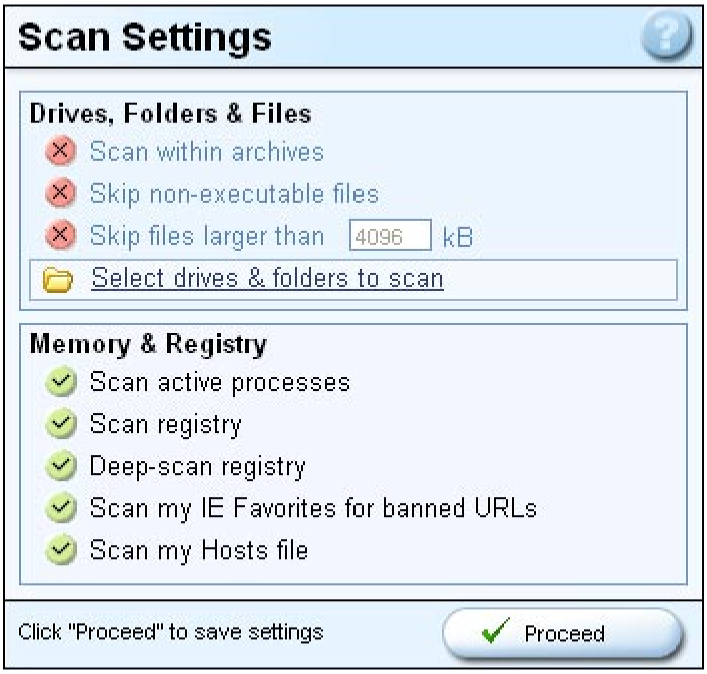
Using definition file: Use the browse feature to locate the folder where the definition file is stored. This setting is very useful for network users. The definition file can be downloaded and stored in a shared or mapped network directory. Using this setup, updates can be managed from a central location

Button

Proceed: Click "**Proceed**" to save your settings and return to the Ad-Aware SE main Status screen.

Note! Clicking the "**Proceed**" button is not required after changing the settings on any given configurations screen if you will be making changes in more than one area. You DO however need to use the "**Proceed**" button to save all changes made when finished with setting your configurations.

4.10.2 Scan Settings



Scan Settings

Drives, Folders & Files

☒ Scan within archives

☒ Skip non-executable files

☒ Skip files larger than 4096 kB

Select drives & folders to scan

Memory & Registry

✓ Scan active processes

✓ Scan registry

✓ Deep-scan registry

✓ Scan my IE Favorites for banned URLs

✓ Scan my Hosts file

Click "Proceed" to save settings

Drives & Folders

Scan within archives: Enables Ad-Aware SE to scan within archives such as .zip, .cab etc. This will increase scanning time

Skip non-executable files: Forces Ad-Aware SE to only scan for executable files. This will lower the scanning time. This option should only be used by advanced users as this will eliminate detection of related content that could cause the removed executables to be reinstalled at a later time

Skip files larger than: "Size of file here" KB: Ad-Aware 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 and will lessen the scanning time.

Select drives & folders to scan: Select the drives and folders you want to scan. You can scan select subsets of a drive or folder. These settings will also be used for automated scanning through the command line.

Memory & Registry

Scan active processes: Ad-Aware scans all active processes currently running on your system.

Scan registry: Ad-Aware scans known Spyware areas of the registry for the current user.

Deep-scan registry: Ad-Aware scans the entire registry for the current user. This will increase the scanning time.

Scan my IE Favorites for banned URLs: Scans the Favorites in Internet Explorer for URLs that are associated with Spyware

Scan my Hosts file: Ad-Aware scans of the hosts file. Edits to the Hosts file are most often used by home page hijackers*

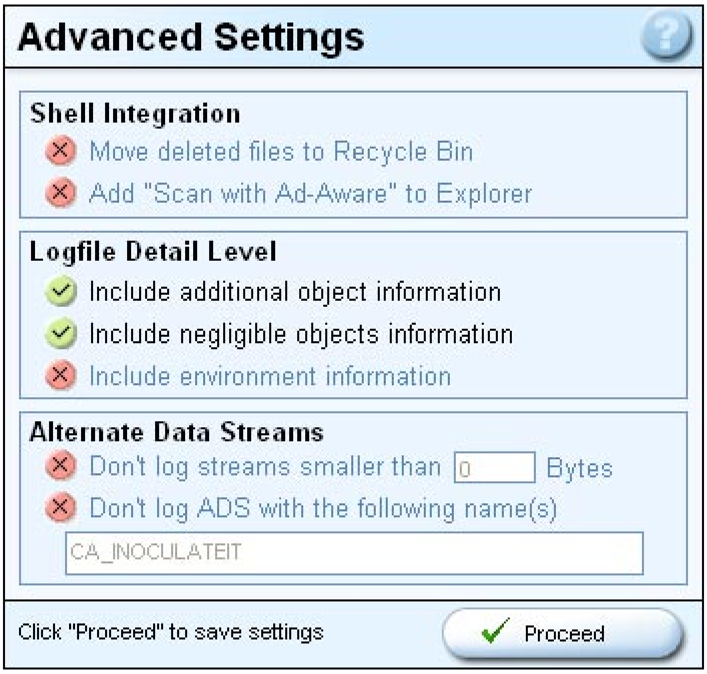
*** Special note to those who use Hosts file blocking!** If you use a Hosts file edit to block content, this option can cause some of these entries to be detected and then presented for removal. Please be sure to review this content at the end of a scan and select those entries that you wish to ignore in subsequent scans with Ad-Aware SE. This will avoid any unwanted changes to your Hosts file.

Button

Proceed: Click "**Proceed**" to save your settings and return to the Ad-Aware SE main Status screen.

Note! Clicking the "**Proceed**" button is not required after changing the settings on any given configurations screen if you will be making changes in more than one area. You DO however need to use the "**Proceed**" button to save all changes made when finished with setting your configurations.

4.10.3 Advanced Settings



Advanced Settings

Shell Integration

☒ Move deleted files to Recycle Bin

☒ Add "Scan with Ad-Aware" to Explorer

Logfile Detail Level

✓ Include additional object information

✓ Include negligible objects information

☒ Include environment information

Alternate Data Streams

☒ Don't log streams smaller than 0 Bytes

☒ Don't log ADS with the following name(s)

CA_INOCULATEIT

Click "Proceed" to save settings

Shell Integration

Move deleted files to Recycle Bin: When removing objects, this option will place the content in the Recycle Bin rather than permanently deleting them. Be aware that if the recycle bin is included in your custom scan settings, these items will be redetected. To avoid endless detections and removals, use this option as a temporary redundant backup for the quarantine archives. When satisfied that the quarantine archive contains all files removed, empty the recycle bin as Ad-Aware SE can replace all files removed to their original locations through the restoration of the applicable quarantine archives

Add "Scan with Ad-Aware" to Explorer: Adds a "**Scan with Ad-Aware**" option to the right click context menu in Explorer. You can right-click on any folder or drive on your computer and scan it with Ad-Aware SE.

Logfile Detail Level

These settings adds additional information to the log file

Include additional object information: Detailed object dependent information will be included in the log file

Include negligible object information: Will add detailed information about detected MRUs to the log file

Include environment information: Will add system related as well as Ad-Aware SE specific environment information to the log file

Alternate Data Streams

NTFS enabled systems only (Win NT, Win 2000, and Win XP)

Don't log streams smaller than "file size here" Bytes: Streams smaller than the specified file size will not be logged

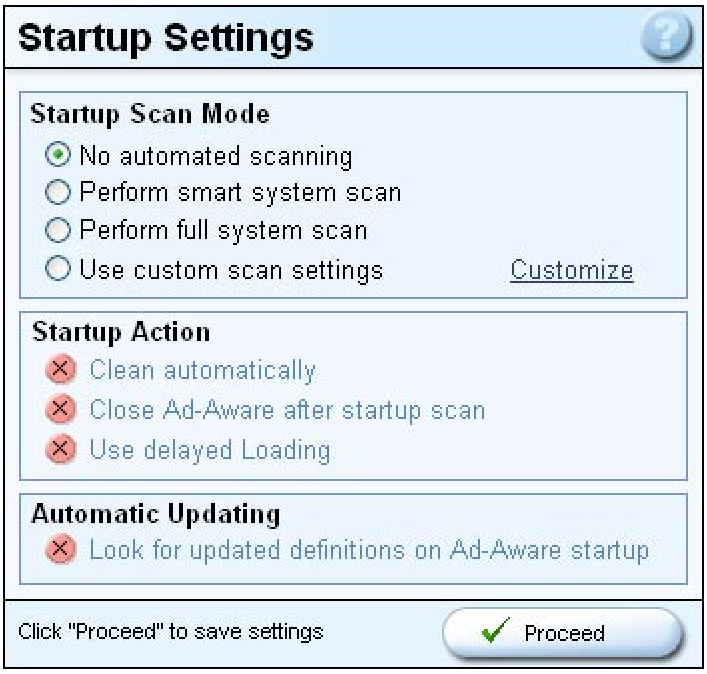
Don't log ADS with the following names: Alternate Data Streams (ADS) with the specified names will not be logged. Values should be comma separated with no space following.

Button

Proceed: Click "**Proceed**" to save your settings and return to the Ad-Aware SE main Status screen.

Note! Clicking the "**Proceed**" button is not required after changing the settings on any given configurations screen if you will be making changes in more than one area. You DO however need to use the "**Proceed**" button to save all changes made when finished with setting your configurations.

4.10.4 Startup Settings



Startup Settings

Startup Scan Mode

● No automated scanning
○ Perform smart system scan
○ Perform full system scan
○ Use custom scan settings

Startup Action

☒ Clean automatically
☒ Close Ad-Aware after startup scan
☒ Use delayed Loading

Automatic Updating

☒ Look for updated definitions on Ad-Aware startup

Click "Proceed" to save settings

Startup Scan mode

No automated scanning: No automated scanning will be performed. This works independently of the command line parameters

Perform smart system scan: A smart system scan will be performed on Windows startup if the proper start up actions are selected (see below)

Perform full system scan: A full system scan will be run on Windows startup if the proper start up actions are selected (see below)

Use custom scan settings: A custom scan will be run on Windows startup if the proper startup actions are selected (see below)

Customize: Takes you to the Scan settings screen where you can customize the scan settings

Startup Action

Clean automatically: If a scan is chosen to be performed above then any objects found will be removed without asking for user confirmation

Close Ad-Aware after startup scan: Once the scan has finished and any detected objects have been handled Ad-Aware SE will shut down automatically

Use delayed loading: This setting is useful when Ad-Aware SE is set to automatically check for definition file updates and scan on startup. To check for updates your computer must be connected to the Internet. On Windows startup it may take a few seconds for your computer to connect to the Internet, depending on what kind of connection you have. Use this delay option to delay the automatic update and scan for 15 seconds.

Automatic Updating

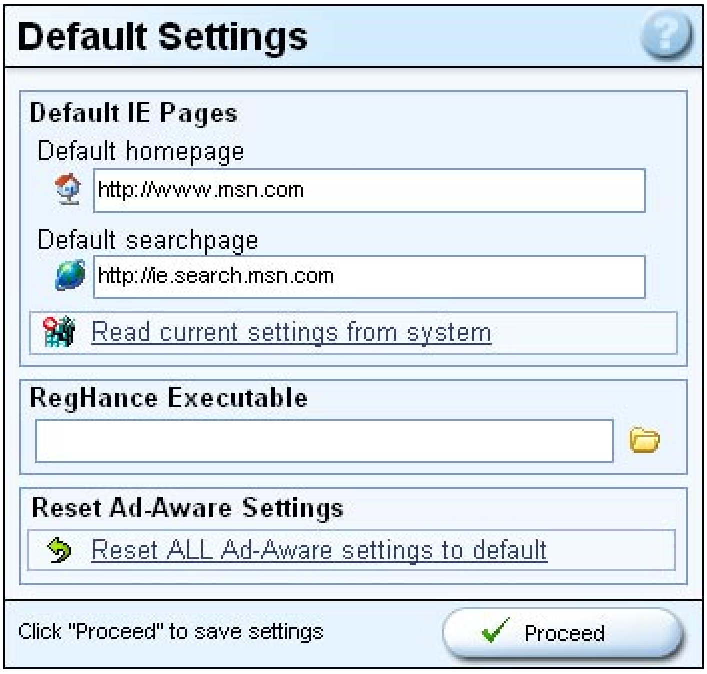
Look for updated definitions on Ad-Aware startup: Automatically checks for updated definition files. If an updated file is available it is automatically downloaded to your computer.

Button

Proceed: Click "**Proceed**" to save your settings and return to the Ad-Aware SE main Status screen.

Note! Clicking the "**Proceed**" button is not required after changing the settings on any given configurations screen if you will be making changes in more than one area. You DO however need to use the "**Proceed**" button to save all changes made when finished with setting your configurations.

4.10.5 Default Settings



Default Settings

Default IE Pages

Default homepage

http://www.msn.com

Default searchpage

http://ie.search.msn.com

Read current settings from system

RegHance Executable

Reset Ad-Aware Settings

Reset ALL Ad-Aware settings to default

Click "Proceed" to save settings

Default IE Pages

Default homepage: Ad-Aware SE uses the defined homepage when recovering from a browser hijack

Default Search Engine: Ad-Aware SE uses the defined search engine when recovering from a browser hijack

Read current settings from system: Changes the default homepage and default search engine entries above to the current settings on your computer. This option is an easy way for you to reset your defaults without having to enter the paths manually

RegHance Executable

Use the browse feature to locate the folder where the RegHance.exe file is installed.

Note! RegHance is an advanced registry editor made by Lavasoft and is a replacement solution for the native registry editor that ships with Microsoft's Windows Operating Systems. It is not included in Ad-Aware SE, but can be purchased from Lavasoft's website. For more information see the chapter Purchasing additional solutions from Lavasoft. The RegHance installer IS however included in the Ad-Aware SE Plus + RegHance and Ad-Aware SE Professional + RegHance bundles

Reset Ad-Aware Settings

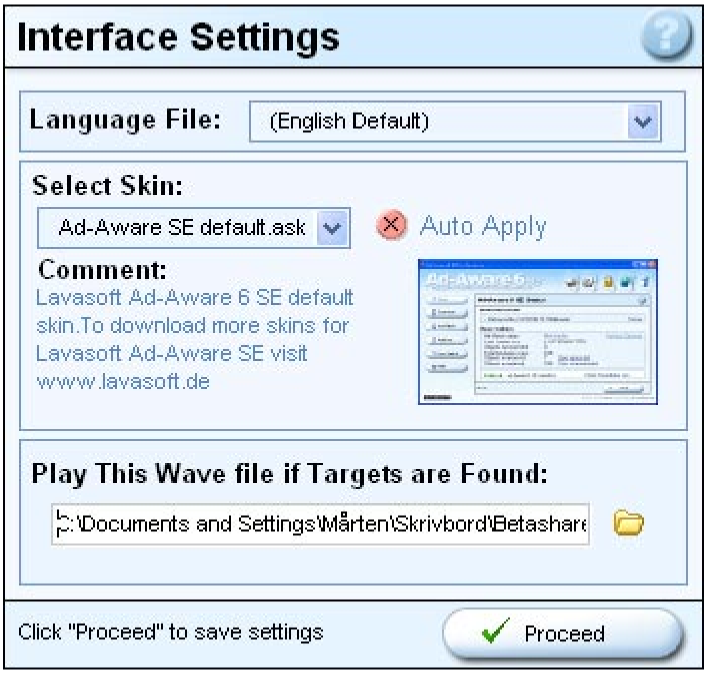
Reset ALL Ad-Aware settings to default: This will reset all Ad-Aware SE settings to the default installation values

Button

Proceed: Click "**Proceed**" to save your settings and return to the Ad-Aware SE main Status screen.

Note! Clicking the "**Proceed**" button is not required after changing the settings on any given configurations screen if you will be making changes in more than one area. You DO however need to use the "**Proceed**" button to save all changes made when finished with setting your configurations.

4.10.6 Interface Settings



Interface Settings

Language File: (English Default)

Select Skin: Ad-Aware SE default.ask

☒ Auto Apply

Comment: Lavasoft Ad-Aware 6 SE default skin.To download more skins for Lavasoft Ad-Aware SE visit www.lavasoft.de

Play This Wave file if Targets are Found: C:\Documents and Settings\Mårten\Skrivbord\Betashare

Click "Proceed" to save settings

Language File

Select your preferred language by locating the flag that corresponds to your country. The interface of Ad-Aware SE will refresh in your chosen language once you click "**Proceed**". You must install the language pack from Lavasoft in order to change the language from those included in the installation. For more information see the Change language chapter

Select Skin

Click in the field to select the skin of your choice. The interface of Ad-Aware will change to reflect the look of that interface once you click "**Proceed**". For more information see the Changing Ad-Aware SE's skin chapter.

Auto Apply: Changes the appearance of Ad-Aware immediately when a new skin is selected. If Auto apply is not selected you must click the "**Proceed**" button to change the appearance. If Auto apply IS activated, Ad-Aware SE will close and then reopen automatically with the new skin applied

Play this Wavefile if Targets are found:

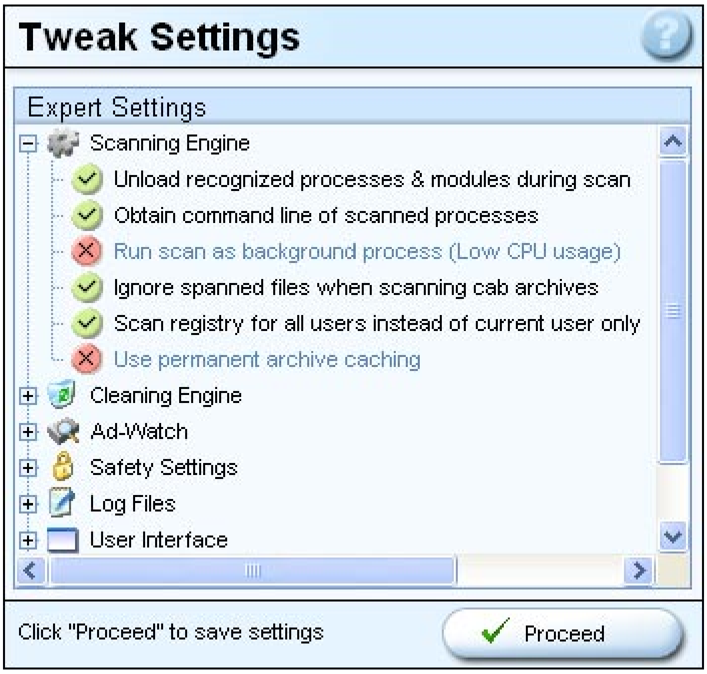
Select a wave-file that will be played when content is detected. Any file with a .wav extension can be used

Button

Proceed: Click "**Proceed**" to save your settings and return to the Ad-Aware SE main Status screen.

Note! Clicking the "**Proceed**" button is not required after changing the settings on any given configurations screen if you will be making changes in more than one area. You DO however need to use the "**Proceed**" button to save all changes made when finished with setting your configurations.

4.10.7 Tweak Settings



Tweak Settings

Expert Settings

- Scanning Engine
  - ✓ Unload recognized processes & modules during scan
  - ✓ Obtain command line of scanned processes
  - ✗ Run scan as background process (Low CPU usage)
  - ✓ Ignore spanned files when scanning cab archives
  - ✓ Scan registry for all users instead of current user only
  - ✗ Use permanent archive caching
- Cleaning Engine
- Ad-Watch
- Safety Settings
- Log Files
- User Interface

Click "Proceed" to save settings

Scanning Engine

Unload recognized processes & modules during scan: This allows Ad-Aware SE to close any currently running process or module that is recognized by Ad-Aware SE's definitions. If this setting is disabled, the recognized process or module will continue to run during the remainder of the scan. Deactivation of this option does not imply that Ad-Aware SE will not be able to remove the executable if selected for removal by the user, just that removal will happen more efficiently if the process has already been stopped

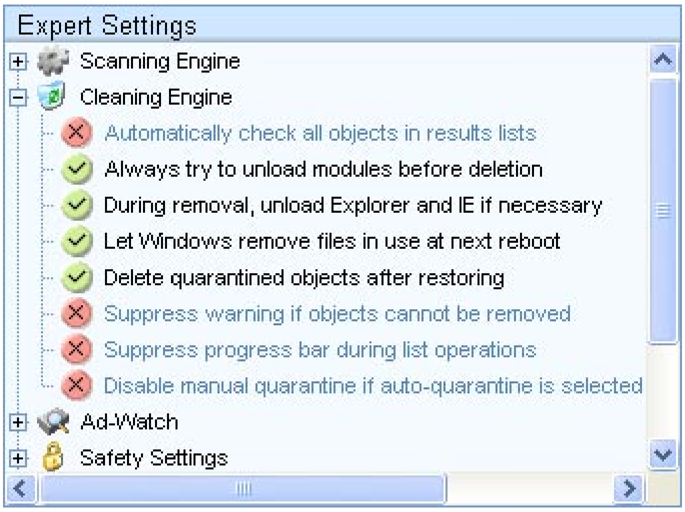
Obtain command line of scanned processes: Ad-Aware SE can determine what command line instructions (including any command line parameters) that were used to start a process. If enabled, this option lists this information in the scan log. If disabled, Ad-Aware SE lists the location of the process executable only

Run scan as background process (Low CPU usage): Forces Ad-Aware SE to run in the background with a lower priority level. This allows for other programs running concurrently with Ad-Aware SE to obtain more processor time

Ignore spanned files when scanning cab archives: Ad-Aware SE skips CAB files which are spanned. Spanned CABs are where several CAB files make up a single CAB archive

Scan registry for all users instead of current user only: Enabling this option will allow Ad-Aware SE to scan the registry sections for the all users', user-specific registry information on the system. If this option is disabled, Ad-Aware SE will scan the currently logged on user's user-specific registry information. In other words, this option will allow you to scan multiple user accounts on a single system rather than having to scan within each user profile separately

Use permanent archive caching: Ad-Aware SE builds a checksum for each archive after scanning it as long as it does not contain any detected objects. During the next scan, it will compare the archive's current checksum against the stored checksum, and only decompress to scan within it again if it has been changed. The checksum changes if the file's contents change in some way. Stored checksums are erased after updating the definitions file to ensure they are scanned against the new definitions.



Expert Settings

- ⊞ Scanning Engine
- ⊟ Cleaning Engine
  - ☒ Automatically check all objects in results lists
  - ✓ Always try to unload modules before deletion
  - ✓ During removal, unload Explorer and IE if necessary
  - ✓ Let Windows remove files in use at next reboot
  - ✓ Delete quarantined objects after restoring
  - ☒ Suppress warning if objects cannot be removed
  - ☒ Suppress progress bar during list operations
  - ☒ Disable manual quarantine if auto-quarantine is selected
- ⊞ Ad-Watch
- ⊞ Safety Settings

Cleaning Engine

Automatically check all objects in results lists: Ad-Aware SE will automatically check all items in the results list

Always try to unload modules before deletion: Ad-Aware SE will try to unload running process modules that match Ad-Aware SE's definitions

Prior to deletion, unloading Explorer and IE if necessary: Windows Explorer, and if necessary Internet Explorer can be unloaded during the removal process. In many cases, items that would normally require a system restart to remove can be removed by Ad-Aware SE without a restart

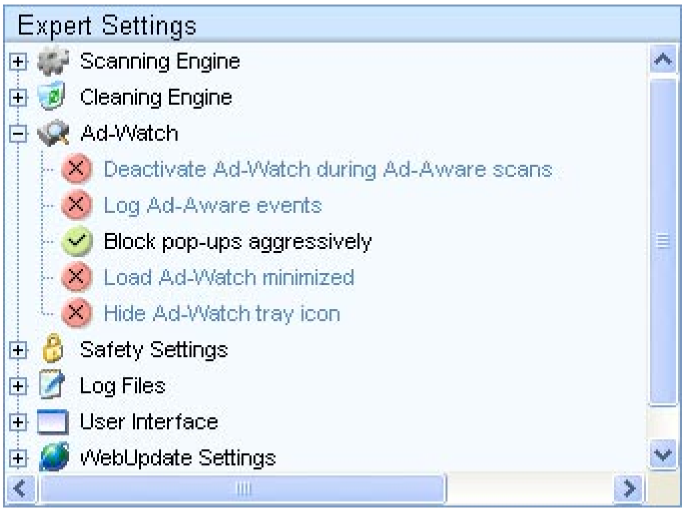
Let Windows remove files in use at next reboot: If a file cannot be removed without a restart, enabling this option will cause Ad-Aware SE to request that the files be removed during the next system restart. If approved, Ad-Aware SE will instruct Windows to remove these files during the restart, and then perform a reboot scan to ensure their removal

Delete quarantined objects after restoring: After the objects in a quarantine file are restored, the quarantine file is deleted. If disabled, the quarantine file will remain on the system even after restoring its contents

Suppress warning if objects cannot be removed: Messages that certain objects cannot be removed will be suppressed. If the "**Let Windows remove files in use at next reboot**" option is enabled, it will automatically do so.

Suppress progress bar during list operations: Disables showing the progress bar during the quarantine and/or deletion process

Disable manual quarantine if auto-quarantine is selected: If the auto-quarantine option is enabled, this option will disable the ability to manually create a quarantine archive



Expert Settings

- ⊞ Scanning Engine
- ⊞ Cleaning Engine
- ⊟ Ad-Watch
  - ✗ Deactivate Ad-Watch during Ad-Aware scans
  - ✗ Log Ad-Aware events
  - ✓ Block pop-ups aggressively
  - ✗ Load Ad-Watch minimized
  - ✗ Hide Ad-Watch tray icon
- ⊞ Safety Settings
- ⊞ Log Files
- ⊞ User Interface
- ⊞ WebUpdate Settings

Ad-Watch

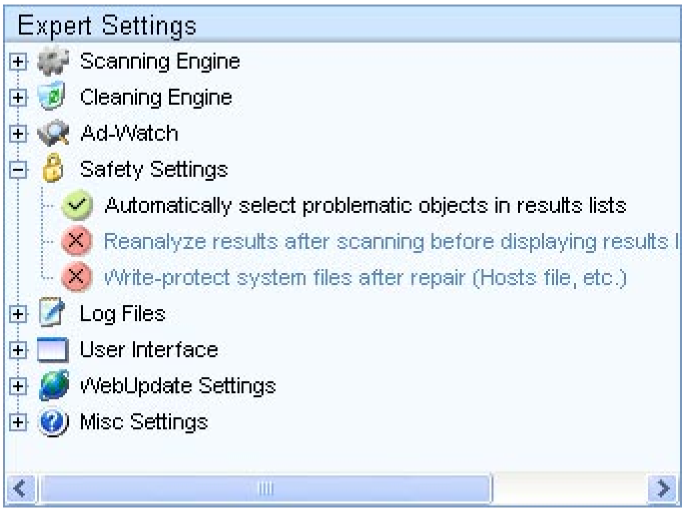
Deactivate Ad-Watch during Ad-Aware scans: Ad-Watch will be deactivated while Ad-Aware SE scans your system

Log Ad-Aware events: Ad-Aware SE events are listed in the Ad-Watch Event log

Block pop-ups aggressively: Ad-Watch blocks pop-ups based on browser window characteristics. It does not rely on sites.txt to determine what to block.

Load Ad-Watch minimized: Ad-Watch will load to the system tray rather than opening when activated

Hide Ad-Watch tray icon: When Ad-Watch is activated the tray icon will not be displayed on your desk top. To make the icon reappear, simply open Ad-Aware SE and deactivate this option. Once the setting has been saved (by clicking the proceed button) the Ad-Watch tray icon will be visible.



Expert Settings

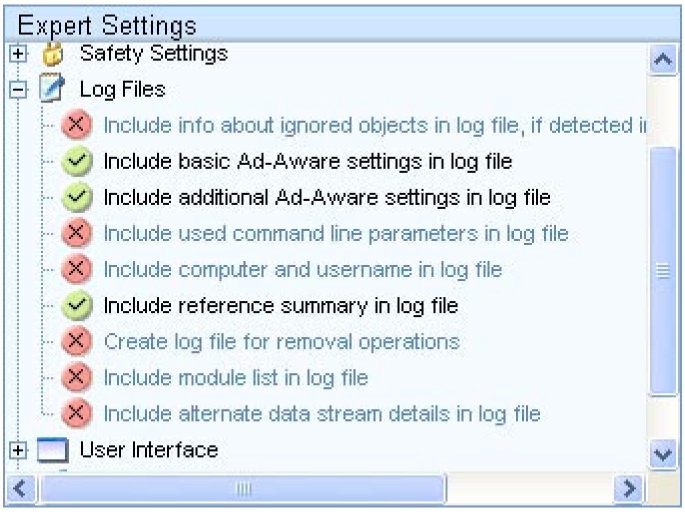
- ⊞ Scanning Engine
- ⊞ Cleaning Engine
- ⊞ Ad-Watch
- ⊟ Safety Settings
  - ✓ Automatically select problematic objects in results lists
  - ✗ Reanalyze results after scanning before displaying results l
  - ✗ Write-protect system files after repair (Hosts file, etc.)
- ⊞ Log Files
- ⊞ User Interface
- ⊞ WebUpdate Settings
- ⊞ Misc Settings

Safety Settings

Automatically select problematic objects in results lists: Ad-Aware SE will automatically select listings which, if not selected, could lead to system instability if other objects are removed and the items appearing in bold are not

Reanalyze result after scanning before displaying result list: After the scan completes, Ad-Aware SE will reanalyze its findings before presenting them

Write-protect system files after repair (Hosts file, etc.): Ad-Aware SE will write-protect certain system files after repairing them, such as the Hosts file



Expert Settings

- ⊞ Safety Settings
- ⊟ Log Files
  - ☒ Include info about ignored objects in log file, if detected i
  - ✓ Include basic Ad-Aware settings in log file
  - ✓ Include additional Ad-Aware settings in log file
  - ☒ Include used command line parameters in log file
  - ☒ Include computer and username in log file
  - ✓ Include reference summary in log file
  - ☒ Create log file for removal operations
  - ☒ Include module list in log file
  - ☒ Include alternate data stream details in log file
- ⊞ User Interface

Logfiles

Include info about ignored objects in logfile, if detected in scan: Ad-Aware SE will list information about detected objects which are in the ignore list in the scan log file

Include basic Ad-Aware settings in logfile: Includes basic settings information in the scan log file

Include additional Ad-Aware settings in logfile: Includes additional settings information in the scan log file

Include used command line parameters in logfile: Includes any command line parameters used to launch Ad-Aware SE in the scan log file

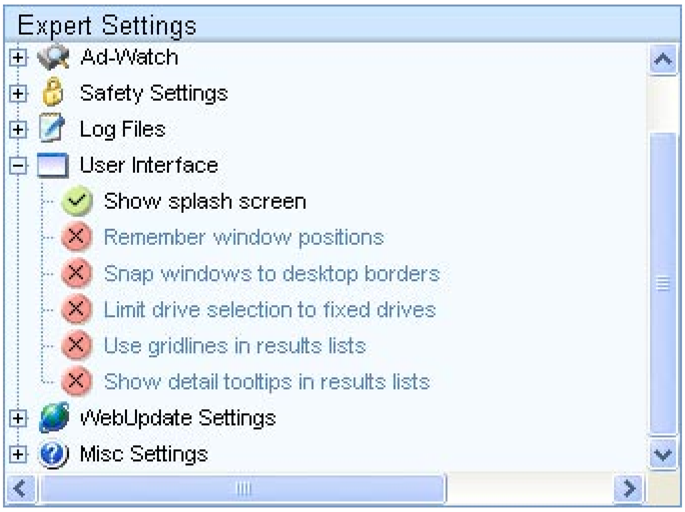
Include computer and username in logfile: Include the computer's name and the username currently logged on in the scan log file

Include reference summary in logfile: Includes a summary of the references detected during the scan and their TAC rating

Create log file for removal operations: Creates a log file for the items removed rather than just detected

Include module list in logfile: Includes the loaded modules for each process in the log file

Include Alternate Data Stream details in logfile: Includes information on any alternate data streams detected during the scan in the log file



Expert Settings

- ⊞ Ad-Watch
- ⊞ Safety Settings
- ⊞ Log Files
- ⊟ User Interface
  - ✓ Show splash screen
  - ☒ Remember window positions
  - ☒ Snap windows to desktop borders
  - ☒ Limit drive selection to fixed drives
  - ☒ Use gridlines in results lists
  - ☒ Show detail tooltips in results lists
- ⊞ WebUpdate Settings
- ⊞ Misc Settings

User Interface

Show splash screen: Ad-Aware SE will show its initialization screen during program startup

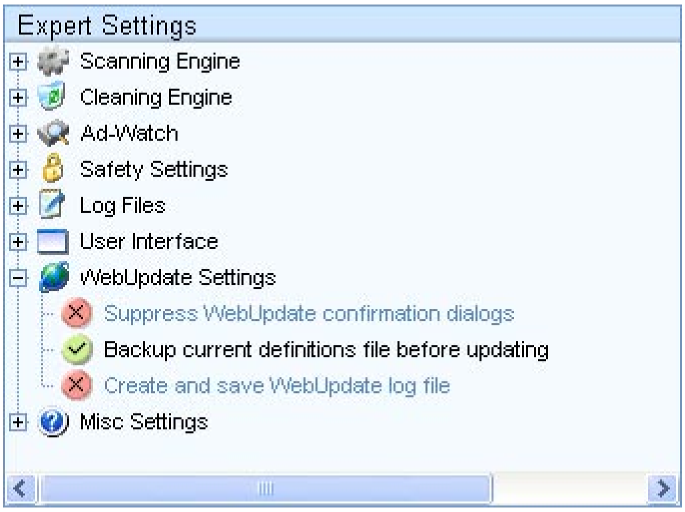
Remember window positions: Ad-Aware SE will remember where it was the last time it was opened

Snap windows to desktop borders: Forces the Ad-Aware SE interface to remain on the desk top. This will prevent the interface from disappearing off the edge if moved too far to the left, right, top, or bottom of the visible work area

Limit drive selection to fixed drives: Ad-Aware SE will only allow fixed hard drives to be selected for scanning

Show gridlines in item lists: Gridlines will appear in the item lists

Show detail tooltips in item lists: Ad-Aware SE will display detailed information when you move your mouse over items in the Ignore, quarantine, and results screens



Expert Settings

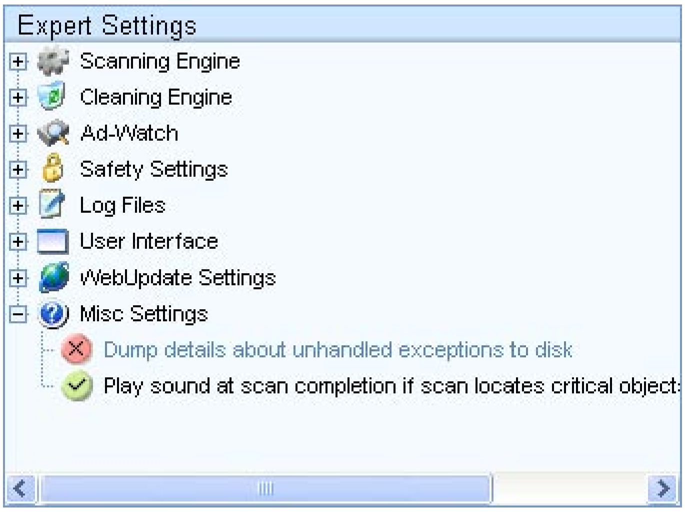
- ⊞ Scanning Engine
- ⊞ Cleaning Engine
- ⊞ Ad-Watch
- ⊞ Safety Settings
- ⊞ Log Files
- ⊞ User Interface
- ⊟ WebUpdate Settings
  - ☒ Suppress WebUpdate confirmation dialogs
  - ✓ Backup current definitions file before updating
  - ☒ Create and save WebUpdate log file
- ⊞ Misc Settings

WebUpdate Settings

Suppress WebUpdate confirmation dialogs: WebUpdate confirmation dialogs will not be shown

Backup current definitions file before updating: Ad-Aware SE will make a backup of the currently loaded definitions file prior to downloading and installing an update

Create and save WebUpdate log file: Ad-Aware SE logs and saves WebUpdate information in a separate log file. This is useful for trouble shooting update problems


Expert Settings
- Scanning Engine
- Cleaning Engine
- Ad-Watch
- Safety Settings
- Log Files
- User Interface
- WebUpdate Settings
- Misc Settings
  - ☒ Dump details about unhandled exceptions to disk
  - ✓ Play sound at scan completion if scan locates critical object:

Misc Settings

Dump details about unhandled exceptions to disk: If an exception occurs that cannot be handled, Ad-Aware SE will append to (or create) a special log file for later trouble shooting and/or product support

Play sound at scan completion if scan locates critical objects: Ad-Aware SE plays a sound at the end of a scan if any critical objects were detected

Button

Proceed: Click "**Proceed**" to save your settings and return to the Ad-Aware SE main Status screen.

Note! Clicking the "**Proceed**" button is not required after changing the settings on any given configurations screen if you will be making changes in more than one area. You DO however need to use the "**Proceed**" button to save all changes made when finished with setting your configurations.

5 Using Ad-Aware SE

5.1 Update the definition file

The definition file is Ad-Aware SE's detection list. It is based on Lavasoft's new Code Sequence Identification (CSI) technology and replaces the reference file used in earlier versions of Ad-Aware.

To make sure your computer is protected the definition file needs to be updated regularly. There are four ways to do this.

WebUpdate*

To start WebUpdate click the WebUpdate button in the toolbar or use the "**Check for updates now**" link on the Status screen. Click "**Connect**" to check if a new definition file is available. If a new file is available click "**OK**" to download it. (The file will automatically be stored to the correct location on your computer.)

Automatic WebUpdate*

You can set Ad-Aware to automatically look for updates and scan on startup. Click the "**Settings**" button in the toolbar and go to Startup Settings. Under WebUpdate check "**Automatically check for updated definition file on startup**". To save your changes click "**Proceed**".

Note! To check for updates your computer must be connected to the Internet. On Windows startup it may take a few seconds for your computer to connect to the Internet, depending on what kind of connection you have. If you have set Ad-Aware to check for updates and scan on Windows startup you should use the "**Use delayed loading**" setting available in the Startup Settings. Use this delay option to delay the automatic update and scan for 15 seconds.

Manual Update*

In some circumstances, you may not be able to update the definition file by using WebUpdate. Reasons can include the server being too busy to process update requests, or proxy settings are not configured correctly in Ad-Aware. You can download the reference file manually using the following steps.

1. Close Ad-Aware
2. Download the latest definition file in a ZIP file from Lavasoft's website*
3. Save it to a temporary location
4. When complete, unzip the contents of the file, either through your favorite ZIP utility or through built-in support in Windows, to the installation directory of Ad-Aware, which is usually C:\Program Files\Lavasoft\Ad-Aware SE Plus\
5. Open Ad-Aware

You can then confirm the latest definition file is installed by looking at the Initialization Status on the main Status screen.

Command Line Parameters*

You can use the command line parameter **+update** to check if a new definition file is available during the initialization of Ad-Aware. If a new definition file is available it will automatically be downloaded and installed.

Example:

```
"C:\Program files\Lavasoft\Ad-Aware SE Plus\Ad-Aware.exe" /smart +update
```

When using this combination of command line parameters Ad-Aware will check for definition file updates and run a smart system scan.

Network Updating

The Professional edition includes mapped and UNC share support. This means that you can use this to store a definitions file update on a remote drive and then configure Ad-Aware SE to load its definitions from an internal location rather than have it seek a new update from our servers. This would require that the updates be downloaded from our servers manually using the download link from our servers. You can then replace the file on the network share or update a test bed copy and then replace the current copy of the file with the update from the test bed copy's directory.

An alternate method is to manually download or update as described above and then, using your native push technology, replace the definitions file in your client distribution.

* You must be connected to the Internet to update the definition file

5.2 Using Command Line Parameters

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

Example:

```
Ad-Aware.exe /smart +silent +update +nice-2
```

Ad-Aware will run silently (without the GUI) in the background, checks for definitions file updates before it performs the scan, and then performs a Smart System scan at high priority.

Available command line parameters

/smart
Performs a Smart System scan

/full
Performs a Full System scan

/custom
Performs a scan using Custom Scanning options predefined by the user

/ads
Performs an ADS (Alternate Data Stream) scan and is only available on NTFS enabled volumes
Using /ads alone will run the ADS scan using the parameters (paths) defined in the scan settings
Using /ads with a path as the very first parameter, for example %Ad-Aware.exe% "C:\test" /ads will run an ADS scan on the defined path

/?
Displays a help window with a listing of all the available command line parameters

/help
Displays help on available command line parameters

/paths:"%pathsfile%"
%pathfile% defines a text file which includes a list with paths that will be scanned. %pathfile% can also specify a remote resource.

/sdump:"%destinationfile%"
Creates a file containing status information at the specified location. This command requires a destination file name. Information appended to the file created will include version, build, loaded definitions file, available add-ons, scanning statistics, etc

+archives
Overrides any archival scan settings so that archives are scanned

-archives
Overrides any archival scan settings so that archives are not scanned

+auto
Performs both scanning and removal in full-automatic mode using the automatic quarantine and log file settings defined by the user

+cskip
Skips the conditional scans

+delay
Activates delayed loading

+diskonly
Only performs a disk scan. It will not perform any memory/registry scans

+log:"%destination%"
Creates a log file at the specified path. The full path name must be added in quotes

+mru
Scans for negligible risk objects and temporarily overrides the last user setting for that option

-mru
Skips the scan for negligible risk objects and temporarily overrides the last user setting for that option

+nice+/-n
"-" boosts priority: AboveNormal, High up to Realtime
(+nice-1 or +nice-2 or +nice-3 respectively)

"+"decreases priority: BelowNormal down to Low
(+nice+1 or +nice+2 respectively)

+nodefnotice
No warning will be given if the definitions file is outdated

+noset
Scan will not alter any user data

+nowrite
Disables all writing to disk. Ignore lists, cache and preferences are not saved if this switch is used

+prefs:"%file%"
Uses a user-defined preference file for the scan. The full path and file name must be added in quotes

+procnuke
Performs an aggressive memory scan. Ad-Aware will try to unload/terminate the process/module and immediately delete it. This is required to handle reciprocal processes for example. It also unloads explorer and recognized modules during the removal, regardless of whether or not the tweak options are set

+ref:"%file%"
Uses user-defined definitions file for the scan. The full path and file name must be added in quotes

+remove:n
n must be a number between 0 and 10. If used in combination with the /auto parameter, only content that has an equal or higher TAC index will automatically be removed

+retv:[out]
Returns the highest TAC rating of all objects found as exit code

+safeload
Loads the minimal configuration required for Ad-Aware SE to operate. Skips loading of cache files, ignore list, plug-ins and extensions. If there are problems launching Ad-Aware SE the conventional

way, use this command.

+sd
Sends command to running instance of Ad-Aware

+silent
Runs Ad-Aware without showing the graphical user interface and scans automatically without removing any detected objects

+update
Checks if a new definitions file is available and downloads it on Ad-Aware SE startup

5.3 Change language

You can change the interface of the program to your language by installing the Language Pack for Ad-Aware SE. The Language Pack is free of charge and can be downloaded from Lavasoft's website.
Download the Language Pack*

Note! Close Ad-Aware before installing the Language Pack!

1. Install the Language Pack.
2. Open Ad-Aware
3. Click the "**Settings**" quick launch button at the top right of the interface
4. Click "**Interface**"
5. Click the arrow to the right of "**Language file**"
6. Select the language of your choice
7. Click "**Proceed**"

More information about which languages are included in the language file can be found here*.

* You must be connected to the Internet to access this link

5.4 Changing Ad-Aware SE's skin

You can change the look of the program by changing skins. Skins are free of charge and can be downloaded from Lavasoft's website. Check for new skins*

1. Open Ad-Aware
2. Click the "**Settings**" quick launch button at the top right of the interface
3. Click "**Interface**"
4. Select a skin in the drop down menu under "**Select Skin**"

The option "**Auto Apply**" changes the appearance of Ad-Aware SE immediately when a new skin is selected. If "**Auto Apply**" is not selected you must click the "**Proceed**" button to change the appearance.

Click "**Proceed**" to save your changes and exit the settings

* You must be connected to the Internet to access this link

5.5 What is the quarantine?

Quarantine files are used to isolate and backup items detected during a scan and gives you the option to reinstall them at a later time.

Items moved to the quarantine folder will be encrypted and compressed, and can only be read and restored using the built in quarantine manager in Ad-Aware SE. Objects stored in quarantine do not pose a threat to your computer.

Note! Any of the objects from the Ad-Aware SE results list can be quarantined, including registry keys, values, data as well as files and folders. Objects can only be quarantined from the Scan Summary, Critical Objects or Negligible Objects lists on the Scanning Results screen.

Adding objects to a quarantine archive

1. Run a scan with Ad-Aware
2. Select the object(s) to quarantine in the Scan Summary, Critical Objects or Negligible Objects lists on the Scanning Results screen
3. Click the "**Quarantine**" button or right click and select "**Quarantine selection**" in the context menu
4. Enter a file name and click "**OK**"
5. A pop-up window showing the number of objects selected for quarantine opens. Click "**OK**" to continue

The quarantine file is now added to the Quarantined Objects list.

Automatically quarantine objects before removal

Ad-Aware SE can be set to automatically quarantine objects prior to removal. Click on the "**Settings**" button in the quick launch toolbar and go to General settings. Check the "**Automatically quarantine objects prior to removal**" setting.

Restore quarantined objects

1. Open the quarantine list by clicking on the quarantine button or the "**Open quarantine list**" link on the Status screen
2. Select the quarantine file you want to restore
3. Right click and select "**Restore selected**" in the context menu or use the "**Restore**" button

5.6 What is the ignore list?

Sometimes you may want to keep a particular detected item installed on your system, and do not want Ad-Aware SE to remove them. In this case you can add the entire product, or the desired components to the ignore list.

Note! Items can only be added to the ignore list from the Scan Summary, Critical Objects or Negligible Objects lists on the Scanning Results screen.

Add objects to ignore list

1. Run a scan with Ad-Aware
2. Select the objects you want to add to the ignore list in the Scan Summary, Critical Objects or Negligible Objects lists on the Scanning Results screen.
3. Right click and select "**Add selected to ignore list**"
4. A pop-up window showing the number of objects that will be added to the ignore list opens. Click "**OK**" to continue

The object is now added to the Ignore list.

Remove objects from the ignore list

1. Open the ignore list by clicking on the "**Open ignore list**" link on the "**Status**" screen
2. Select the object you want to remove
3. Right click and select "**Remove selection from ignore list**" in the context menu or use the "**Remove**" button

5.7 Setting up Ad-Aware SE

To keep your computer protected it is important that you update the definition file and run scans on a regular basis. You can set up Ad-Aware to automatically update the definition file, scan, quarantine detected objects and clean your computer on Windows startup. To set up the automation follow the step-by-step instructions below.

1. Click the "**Settings**" button in the toolbar and click the "**Startup**" button

Automatic WebUpdate*

2. Select "**Automatically check for updated definitions on startup**" in the Auto-Updating section

Automatic Scans

3. Select a scan mode in the Startup Scan Mode section

Automatic Cleaning

4. Select "**Clean automatically**" in the Startup Action section

Automatic Quarantine

5. Click the "**General**" button to go to General Settings
6. Select "**Automatically quarantine objects prior to removal**" in the Safety Settings section

7. To save your changes click "**Proceed**".

* You must be connected to the Internet to update the definition file

5.8 Performing your first scan

Before you scan your computer with Ad-Aware SE for the first time you should run WebUpdate to make sure that you have the latest definition file. It is also recommended to have Ad-Aware set to automatically quarantine files prior to removal. Click on the "**Settings**" button in the quick launch toolbar to open the General settings screen. Check the "**Automatically quarantine objects prior to removal**" setting and then click "**Proceed**" to save your changes.

When this is done you are ready to perform your first scan. Click the "**Scan now**" button in the main menu on the left side of the main status screen or use the "**Start**" button in lower right corner. This will open the Preparing System Scan screen. Select "**Perform Full System scan**" and click "**Next**" to start your first scan.

After the scan is completed you will be presented with a detailed listing of the items that were detected. Please be sure to review each item that has been presented in the results screen before removing them. Ad-Aware is designed to report possible suspicious content present on your system and to allow you a simple method for removing it should you so decide. We do not suggest or recommend that everything detected by Ad-Aware should be removed; it is up to you the user to make that decision. We understand that this may be a difficult task; therefore we have developed TAC which stands for Threat Assessment Chart. More information is available in the Threat Assessment Chart - TAC chapter.

If you have decided to keep one or more items, select them from the Scanning Results lists (be sure to unselect other content you wish to remove) and right click the entry to open the context menu. Either select each item individually for each component to be ignored, or use the selection options in the context menu. Select the "**Add selection to ignore list**" to add this content to your ignore list. Ad-Aware will not display these items in the scan results when you perform scans in the future.

Once this content has been added to your ignore list you will be taken back to the scan results screen where you can repeat the above process as required, to not select anything more (all items are unchecked), or to remove the content as you deem appropriate.

Click the "**Next**" button on the Scan Complete screen to view the Scanning Results. Select the objects you want to remove by selecting them in the scan results lists or right click to select multiple items by using the context menu. Click "**Next**" and then "**OK**" in the pop-up window to confirm the removal.

5.9 Automated scans

There are three distinct ways for you to automate Ad-Aware SE

Simple Startup Scan

This method makes use of the Startup Settings to configure Ad-Aware to perform a scan at Windows startup.

To do this click the "**Settings**" button in the quick launch toolbar and go to "**Startup Settings**". Select the appropriate scan mode in the "**Startup Scan Mode**" section,

No automated scanning: No automated scanning will be performed. This works independently of the command line parameters
Perform smart system scan: A smart system scan will be performed at Windows startup if the proper Startup Actions are selected (see below)
Perform full system scan: A full system scan will be run at Windows startup if the proper Startup Actions are selected (see below)
Use custom scan settings: A custom scan will be run at Windows startup if the proper Startup Actions are selected (see below)

And then choose the appropriate Startup Actions

Clean automatically: If a scan is chosen to be performed above then any objects found will be removed without asking for user confirmation
Close Ad-Aware after startup scan: Once the scan has finished, and any detected objects have been handled, Ad-Aware SE will shut down automatically
Use delayed loading: This setting is useful when Ad-Aware SE is set to automatically check for definition file updates and scan on startup. To check for updates your computer must be connected to the Internet. On Windows startup it may take a few seconds for your computer to connect to the Internet, depending on what kind of connection you have. Use this delay option to delay the automatic update and scan for 15 seconds.

Additionally you can also choose to automate the definitions file update so you are assured that it is up to date

Look for updated definitions on Ad-Aware startup: Automatically checks for updated definition files. If an updated file is available it is automatically downloaded to your computer. This option could fail if your computer is slow to boot or if it takes too long to load your Internet connection at startup. If you experience any difficulties you can use the delayed loading option as described above

Windows Task Scheduler

You do not have to use the Windows Startup Scan to automate Ad-Aware SE. Instead you can specify the time and date of your scanning by using a simple but powerful feature of Windows; the Windows Task Scheduler. This is an excellent way for you to perform routine daily, weekly, and monthly scans

Open the Task Scheduler and then select the "**Add Scheduled Task**" icon. Follow the wizard and when appropriate, enter the required command line parameter. For more information see the chapter Using Command Line Parameters.

Example:

```
"%programfiles%\Lavasoft\Ad-Aware SE Professional\Ad-Aware.exe" /smart +silent
+update +nice-2
```

Ad-Aware will run silently (without the graphical user interface) in the background, check for a definitions file update before it performs the scan, and then performs a Smart System scan at IDLE priority

Advanced Automation

Ad-Aware SE can be automated using Batch and script. The command line parameters available with Ad-Aware can be found in the chapter Using Command Line Parameters.

Example: Batch file

```
@ECHO OFF

"%programfiles%\Lavasoft\Ad-Aware SE Professional\Ad-Aware.exe" /full +update
+auto
```

This batch file makes Ad-Aware check for definition file updates, runs a full system scan and automatically removes all detected objects.

Example: Script

```
Set WshShell = WScript.CreateObject("WScript.Shell")
Set env = Wshshell.Environment("Process")

Ad-Awarecmd = chr(34) & env("PROGRAMFILES") & "\Lavasoft\Ad-Aware SE Plus\Ad-
   Aware" & chr(34)
rc = WshShell.Run(Ad-Awarecmd & " /full +update +auto", 0, True)
```

5.10 Virus warnings while performing a scan with Ad-Aware

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

Most antivirus resident scanners will not scan compressed files and only monitor your memory for the sign of an active viral process. During a scan, Ad-Aware will temporarily decompress files to scan their contents without activating the content, but in doing so, the file is noticed by the antivirus' resident scanner. Also, some antivirus applications include an option to quarantine infected files, and when Ad-Aware decompresses these quarantined files, the antivirus background scanner detects the virus moving outside the quarantine area. To avoid this you can either remove the quarantined files via your antivirus application, or have Ad-Aware ignore the antivirus program's quarantine folders/files during a scan.

6 What are add-ons?

Add-ons are designed to enhance and extend the functionality that Ad-Aware provides for your system. They aren't strictly necessary for Ad-Aware to perform its core purpose, but they can add an extra layer of control to the user. They can stop potentially dangerous Windows services, provide additional information about suspicious content, and turn off certain annoyance Windows features.

There are three types of add-ons: tools, extensions and statistics.

Tools are stand-alone programs that can be used without performing a scan.
Extensions provide more information about the objects detected by Ad-Aware and offer more options for handling them. Extensions are connected to the detected objects and can only be used by right-clicking an object in the Scan result detailed view or in Process-Watch.
Statistics is a preinstalled add-on that shows information about previous scans.

The tools and extensions can be found on the Add-ons screen. To run a tool select it in the Add-ons list and then click the "**Run plug-in**" button. Extensions can only be used when a scan has finished or from within the Process-Watch right click context menu.

6.1 Download, install & run add-ons

You can download add-ons free of charge from our website. Look for add-ons and extensions.*

Installing a plug-in is simple. After you've downloaded a plug-in and closed Ad-Aware, extract the installation executable from the archive and run the downloaded file. The installer will handle finding your Ad-Aware plug-in folder and automatically install it for you. The next time you run Ad-Aware, click on the "**Add-ons**" button to use your installed plug-ins.

* You must be connected to the Internet to access this link

Download

1. Go to the Lavasoft add-ons page*
2. Select the appropriate add-on in the list to the right of that page and click on its link
3. Carefully read the add-on information on the website. Note if there are any specific steps to be taken for that add-on to work
4. At the bottom of the page you will find a download link. Click it
5. A window should appear asking you to save the file. Make note of the name of the file
6. Click "**Save**" and browse to your "**My Documents**" folder, then click "**Save**" again
7. The download should commence

Install

1a. Once the download is finished, if asked, click "**Open**" to execute it
1b. If you were not presented with the "**Open**" choice then browse to your "**My Documents**" folder and locate the file you downloaded (extension might not be shown). Doubleclick to execute it.
2. An installation Wizard will open. Follow the instructions in the installation wizard to install the add-on

Run

Tools
To run a tool, select it in the Tools list and click the "**Run tool**" button. You can also start a tool by doubleclicking it.

Extensions
An extension is connected to the detected objects and can only be used after scanning is completed. The installed extensions are shown in the Extensions list and are available under "**Extensions**" in the context menus. Select one or more objects in one of the Scanning Results lists. Click the right mouse

button and select the extension you want to use.

6.2 How to uninstall Add-ons for Ad-Aware SE

All add-ons installed on your computer will be removed if you uninstall Ad-Aware. If you wish to uninstall an add-on without removing Ad-Aware, follow the step-by-step instructions below

1. Close Ad-Aware
2. Click the Windows "**Start**" button
3. Go to "**Control Panel**"
4. Click "**Add/remove Programs**"
5. Locate the name of the add-on you wish to remove
6. Click "**Change/remove**"
7. Click "**Next**" on the window which appears
8. Click "**Finish**"

The add-on is now removed.

7 What is Ad-Watch?

Ad-Watch is the real time monitor included in the Ad-Aware SE Plus and Professional packages. Ad-Watch goes beyond what other security suites offer by adding another layer of protection to your system proactively. It runs silently in the background, watching for Malware/parasites that try to install on or modify your system.

While Ad-Aware SE detects and cleans your system from known Malware and advertising parasites, Ad-Watch goes even further by catching these programs before they can integrate into your system. If Malware/parasites are detected, Ad-Watch pops up, unloads the particular module and launches Ad-Aware. You can change the action taken by Ad-Watch in the options menu. There are additional settings in Ad-Aware SE in the Tweak Options.

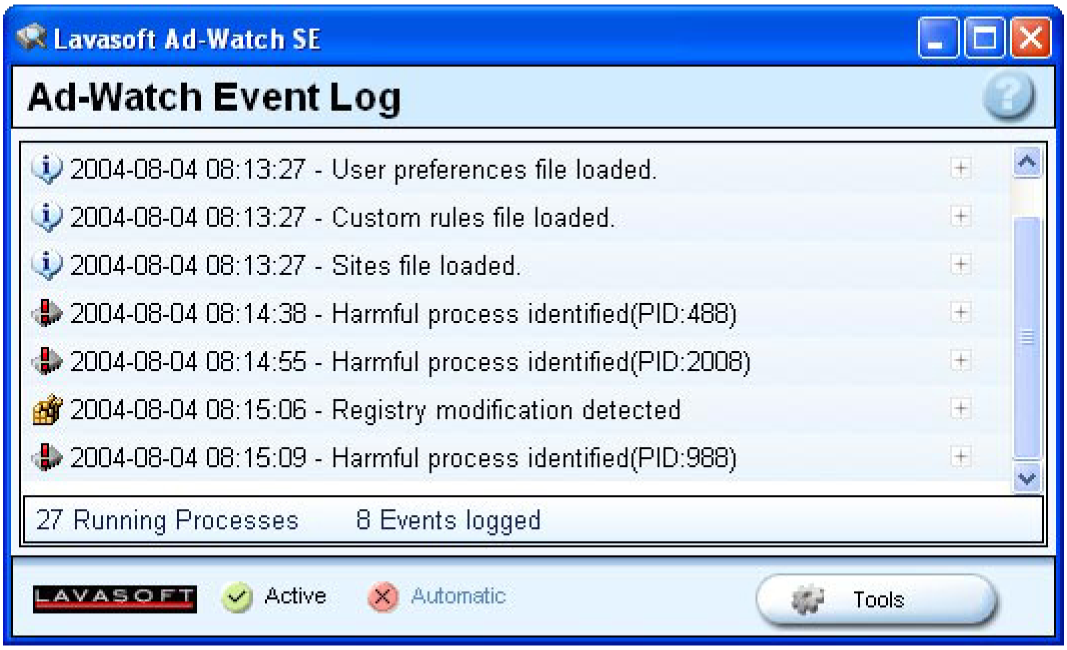
You can lock the startup sections of your registry, block possible and actual browser hijack attempts, block suspicious processes, lock executable file associations, Block malicious cookies, block Pop-ups, and uses the all new CSI technology to protect you from unknown variants as well. Even if Ad-Watch is turned off and something DOES install onto your system, it will recognize it and will kill the process as soon as it has seen it when turned back on.

Ad-Watch will also enable you to continue using detectable processes through its filtering technology. This is accomplished simply by placing Ad-Watch in manual blocking mode and then, when Ad-Watch alerts to the applicable process, select the "Allow" button in the Popup warning. The process has now been added to Ad-Watch's filter list which can be accessed by clicking the "Filter" button on the tool screen. In addition, we have also included a rules editor that will allow you to pre-allow changes to your registry when installing other software applications or when making frequent profile changes.

Note! Ad-Watch shares the definition file with Ad-Aware

7.1 Ad-Watch Event Log

The window will list all events that Ad-Watch has logged during the session.



```
2004-08-04 08:13:27 - User preferences file loaded.
2004-08-04 08:13:27 - Custom rules file loaded.
2004-08-04 08:13:27 - Sites file loaded.
2004-08-04 08:14:38 - Harmful process identified(PID:488)
2004-08-04 08:14:55 - Harmful process identified(PID:2008)
2004-08-04 08:15:06 - Registry modification detected
2004-08-04 08:15:09 - Harmful process identified(PID:988)
27 Running Processes    8 Events logged
```

Running Processes: Shows the number of processes currently running

Tip! If you place your mouse cursor over this area, you will be presented with a list of the processes currently running on your system

Events logged: Shows the number of Events that Ad-Watch has reported during the session.

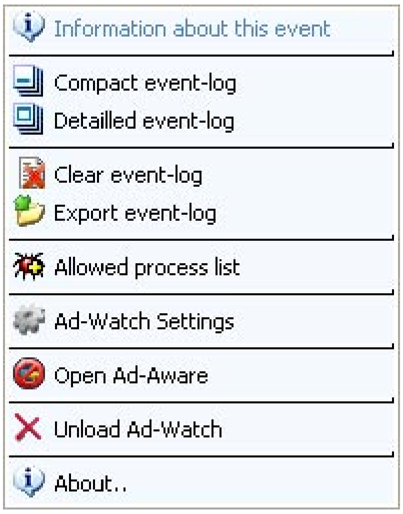
Options

Active: This will turn Ad-Watch On\Off without closing it
Automatic: All suspicious activity will be blocked automatically

Buttons

?: Show quick help for Ad-Watch
Tools: Switches to the Tools & Preferences screen

Right click any entry in the Ad-Watch Event Log window to access the context menu



Context menu

Information about this event: this will take you to our web site where more information will be displayed for the chosen event

Compact event-log: this will collapse all event log entries to a single line
Detailed event-log: all entries in the event log will be expanded to show the event details

Clear event-log: this will clear all entries from the Ad-Watch event log window. **Note!** This will NOT clear the event history log file
Export event-log: this will save a copy of the event log in text format. You will need to name the file and choose the location for it to be saved

Allowed Process list: this will open the Ad-Watch Filter screen in the Tools & Preferences section

Ad-Watch Settings: opens the Options screen in the Tools & Preferences section

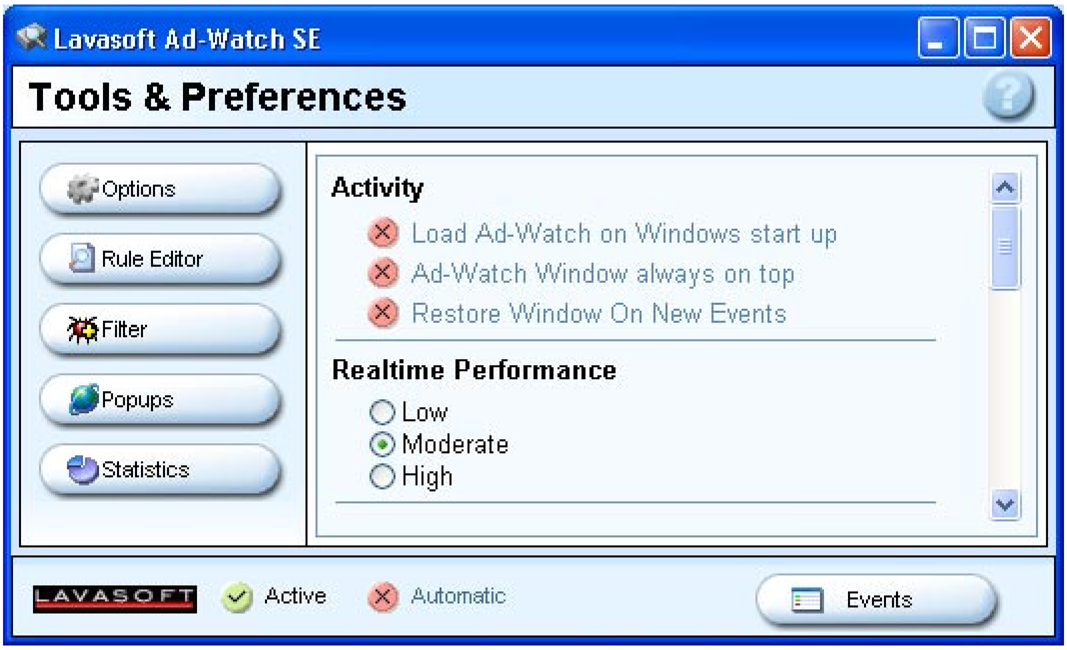
Open Ad-Aware: this will start Ad-Aware

Unload Ad-Watch: this will terminate Ad-Watch

About: Will open a pop-up window with the Ad-Watch build and copyright information

7.2 Tools & Preferences

In an effort to make Ad-Watch both easier to use and to configure, we have separated most of the Ad-Watch configurations and placed them within the Ad-Watch user interface (UI). We have also added two new features (see below)



Activity

☒ Load Ad-Watch on Windows start up
☒ Ad-Watch Window always on top
☒ Restore Window On New Events

Realtime Performance

○ Low
● Moderate
○ High

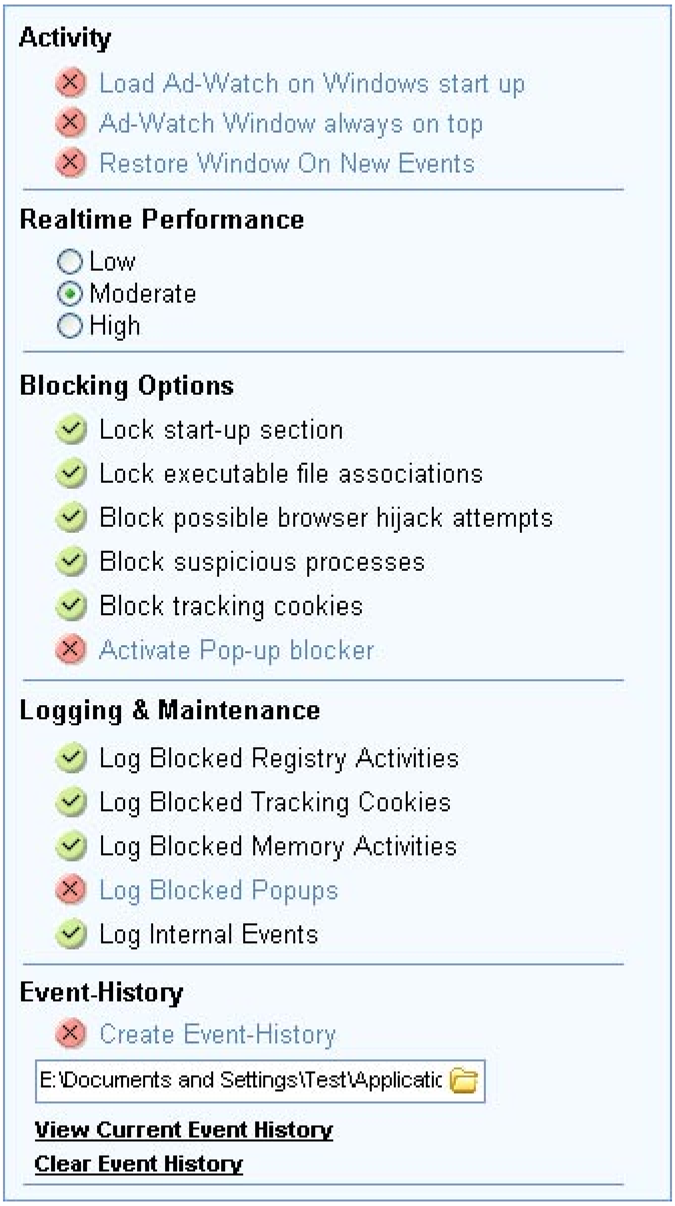
✓ Active ☒ Automatic

Buttons
?: show quick help for Ad-Watch
Events: Switches to the Ad-Watch Event Log screen

Options: Takes you to the Options screen
Rule Editor: Takes you to the Rule Editor
Filter: Takes you to the Filter screen
Pop-ups: Takes you to the Pop-ups screen
Statistics: Takes you to the Statistics screen

Active: This will turn Ad-Watch On\Off without closing it
Automatic: Suspicious activity will be blocked automatically

7.2.1 Options



Activity

- ✗ Load Ad-Watch on Windows start up
- ✗ Ad-Watch Window always on top
- ✗ Restore Window On New Events

Realtime Performance

- ○ Low
- ● Moderate
- ○ High

Blocking Options

- ✓ Lock start-up section
- ✓ Lock executable file associations
- ✓ Block possible browser hijack attempts
- ✓ Block suspicious processes
- ✓ Block tracking cookies
- ✗ Activate Pop-up blocker

Logging & Maintenance

- ✓ Log Blocked Registry Activities
- ✓ Log Blocked Tracking Cookies
- ✓ Log Blocked Memory Activities
- ✗ Log Blocked Popups
- ✓ Log Internal Events

Event-History

- ✗ Create Event-History

E:\Documents and Settings\Test\Applicatic

Activity

Load Ad-Watch on Windows start up: If activated, Ad-Watch will start with Windows
Ad-Watch Window always on top: This option will force the Ad-Watch event log to stay on top of all other open windows when restored
Restore Window on new events: This will cause the Ad-Watch event log window to open only if a new event has been detected

Realtime Performance

These settings do not imply that Ad-Watch will not protect your system with lower priority levels, just that the frequency of background scans will be fewer. The lower settings are appropriate for older systems or those with limited resources. Adjust according to your requirements and preferences

Low: Ad-Watch will monitor your system with the lowest priority level
Medium: Ad-Watch will monitor your system with a normal priority level
High: Ad-Watch will monitor your system with the highest priority level

Blocking Options

Lock Start-up sections: The start up (run) sections of the registry will be locked. No changes will be permitted
Lock Executable File Associations: Blocks (only) the most common associations (used by worms and viruses) so that they cannot stealthily change executable, shortcut, and registry file associations
Block Possible Browser Hijack Attempts: Stops suspicious files from attaching to and taking over the browser
Block Suspicious Processes: Ad-Watch will block all suspicious processes on the system
Block Tracking Cookies: Ad-Watch will block known tracking cookies. If Ad-Watch is turned off and known tracking cookies are installed, when you next activate Ad-Watch these cookies will automatically be detected and deleted (blocked)
Activate Pop-up blocker: The popup blocking capability in Ad-Watch will be turned on

Logging & Maintenance

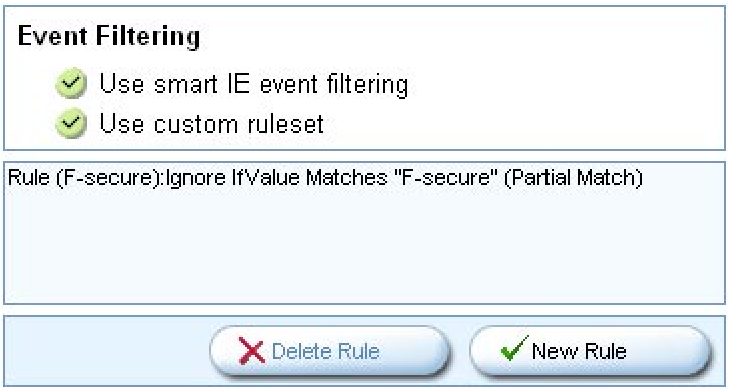
Log Blocked Registry Activities: Attempted changes to your registry will be shown in the event log window. If Event History logging is active, the event(s) will be appended to the Event History log (see Event-History below)
Log Blocked Tracking Cookies: Blocked tracking cookies will be shown in the event log window. If Event History logging is active, the event(s) will be appended to the Event History log (see Event-History below)
Log Blocked Memory Activities: Blocked processes will be shown in the event log window. If Event History logging is active, the event(s) will be appended to the Event History log (see Event-History below)
Log Blocked Pop-ups: All pop-ups blocked will be shown in the event log window. If Event History logging is active, the event(s) will be appended to the Event History log (see Event-History below)
Log Internal Events: Ad-Watch initialization information will be shown in the event log window. If Event History logging is active, the event(s) will be appended to the Event History log (see Event-History below)

Event-History

Create Event-History: Creates a continuous log of blocked content (as configured above) in the specified location
View Current Event History: Opens the Event History log
Clear Event History: Clears the contents of the Event History log

7.2.2 Rule Editor

By defining rules the user can configure Ad-Watch to pre-allow changes to the registry. You can set up rules to allow certain registry keys and/or registry values to be changed



Event Filtering

✓ Use smart IE event filtering

✓ Use custom ruleset

Rule (F-secure):Ignore IfValue Matches "F-secure" (Partial Match)

Options

Event Filtering

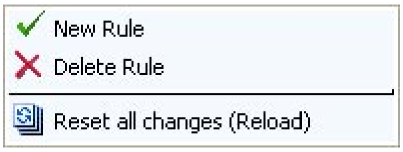
Use smart IE event filtering: Ad-Watch ignores/allows standard IE events which occur whenever any IE setting changes such as font size, toolbar layout etc.

Use custom ruleset: Ad-Watch uses rules defined by the user. This can be used with the smart filtering option

Buttons

Delete Rule: Deletes the selected rule
New Rule: Opens the dialog window Add New Rule where you can create new rules

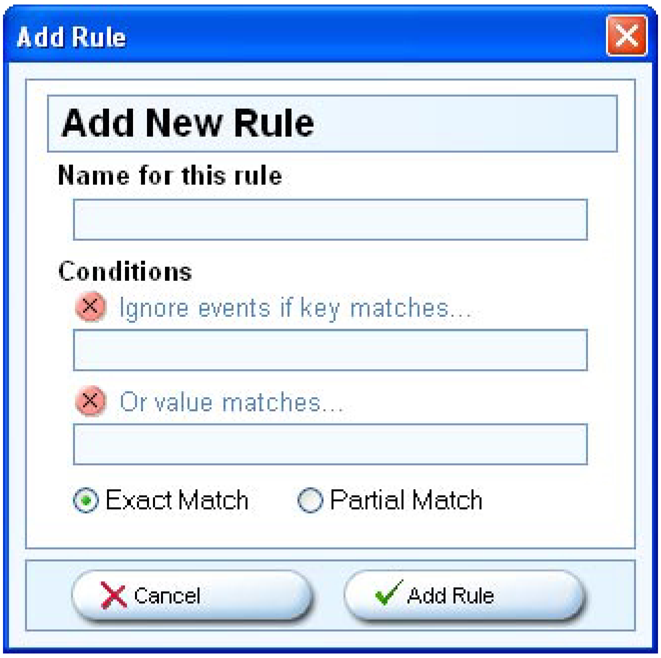
Right-click to open the context menu where more options are available



Context menu

New Rule: Opens the dialog window Add New Rule where you can create new rules
Delete Rule: Deletes the selected rule
Reset all changes (Reload): Resets all changes made to the rules list. A confirmation window will open allowing you to continue or cancel the action.

7.2.2.1 Add New Rule



Name for this rule: Enter name of the rule here

Conditions for this rule
Ignore events if key matches: Enter a registry key
Or value matches: Enter a registry value

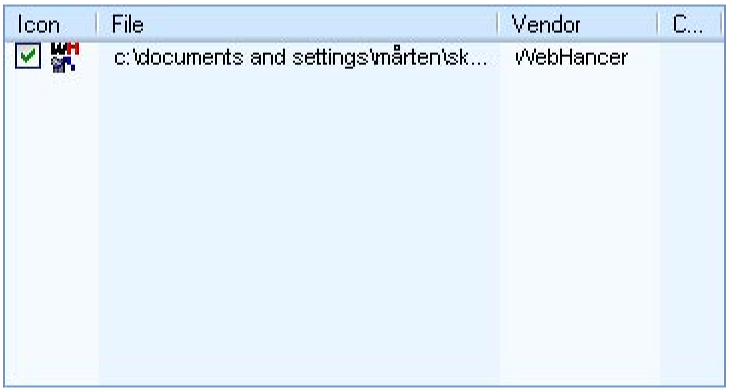
Exact Match: The registry key or value must match exactly
Partial Match: Only a part of the registry key or value must match

Buttons

Cancel: Exit the "**Add New Rule**" window without making a new rule
Add Rule: Add the rule to the rule list

7.2.3 Filter

This is where the processes are listed if you choose to allow them when they are reported by Ad-Watch.



Icon	File	Vendor	C...
☑	c:\documents and settings\mårten\sk...	WebHancer	

Note! You must have the Automatic setting disabled before the Allow or Block options will be available when Ad-Watch reports an event

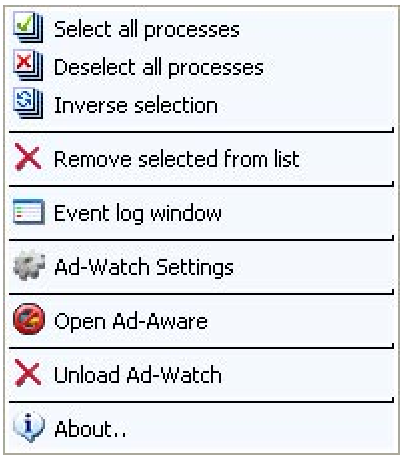
The Processes are listed by: Icon, File, Vendor and a brief Comment.
You can manage them by highlighting an entry and right clicking in the window.

If you have a program that attempts to load a process in the computer's memory and is on the target list, it will be blocked unless you set Ad-Aware and Ad-Watch up like this:

1. Double click the Ad-Watch Tray Icon to open the Ad-Watch window
2. Uncheck the "**Automatic**" button
3. Go to the Ad-Watch options, make sure that "**Block suspicious processes**" is checked
4. Click "**Proceed**"
5. Launch the program you want to allow. If suspicious activity, i.e. a memory process of a targeted object attempting to load is detected a warning will appear. You will then be allowed to choose to Block or Allow that process
   a. To allow the process click "**Allow**". Allowed processes will be added to the Ad-Watch Filter list
   b. To deny or block the process click "**Block**".

Note! Registry changes are not added to the filters list.

Right-click to open the context menu where more options are available



Context menu

Select all processes: Selects all listed processes
Deselect all processes: Deselects all listed processes
Inverse selection: Inverses the selection

Remove selected from list: Removes the selected process from the list

Event log window: Takes you to the Event log screen

Ad-Watch Settings: Takes you to the Ad-Watch Options screen

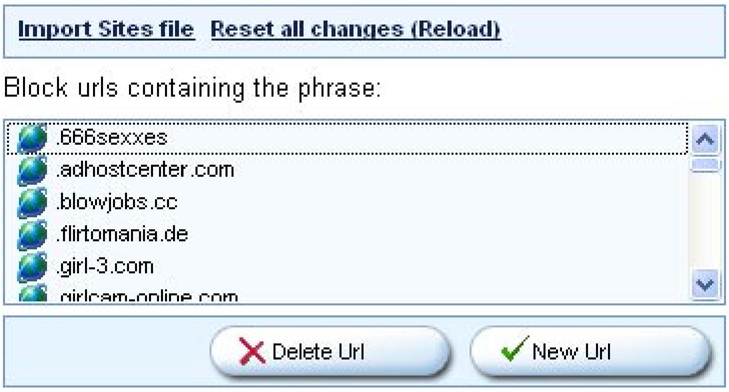
Open Ad-Aware: Opens Ad-Aware if it is not already open

Unload Ad-Watch: Terminates Ad-Watch

About: Shows information about Ad-Watch

7.2.4 Pop-ups

This is the "black list" of websites that Ad-Watch blocks. The URLs are stored in the sites.txt file in your Ad-Aware SE directory.



.666sexxes
.adhostcenter.com
.blowjobs.cc
.flirtomania.de
.girl-3.com
.girlcam-online.com

The popup blocking is designed to be user configurable and sites can easily be added to or removed from the sites list. You can also create a custom sites file in Notepad. The file should contain one partial or full domain name per line. You cannot put two domains on the same line. Also when manually editing the sites.txt file or creating a custom file, do not use the enter key at the end of the edited line

Tip! If there is a site that you do not want to be viewed on the computer, add the URL of that site to the sites list. This can be useful for Parental Blocking, etc

Links

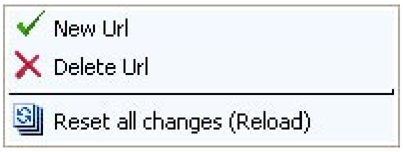
Import sites file: this will import a custom user defined sites file that will be added to the sites list
Reset all changes (Reload): this will remove all changes made during the current session and reset the sites list to its previous configuration. This is only per session and will not reset the list to the installation default. A confirmation window will open allowing you to continue or cancel the action

Block URL's containing the phrase: Shows all sites included in the sites list. Select and click on an entry to edit it

Buttons

Delete URL: Delete the selected URL from the site list
New URL: Opens a dialog window where you enter a partial or complete URL. Click on "**Add URL**" to include it in the site list.

Right-click to open the context menu where more options are available

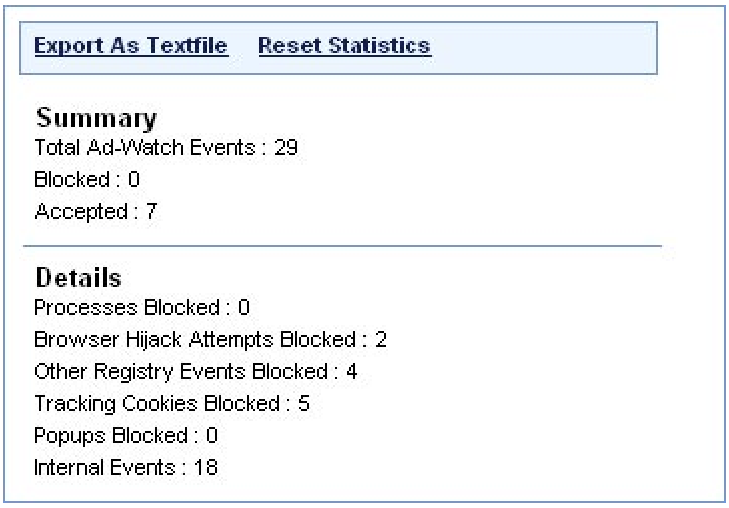


Context menu

New URL: Opens a dialog window where you enter a partial or complete URL. Click on "**Add URL**" to include it in the site list.
Delete URL: Delete the selected URL from the site list
Reset all changes (Reload): this will remove all changes made during the current session and reset the sites list to its previous configuration. This is only per session and will not reset the list to the installation default. A confirmation window will open allowing you to continue or cancel the action.

7.2.5 Statistics

Shows the total statistics for Ad-Watch blocking and filtering



Summary
Total Ad-Watch Events : 29
Blocked : 0
Accepted : 7

Details
Processes Blocked : 0
Browser Hijack Attempts Blocked : 2
Other Registry Events Blocked : 4
Tracking Cookies Blocked : 5
Popups Blocked : 0
Internal Events : 18

Summary

Total Ad-Watch Events: Total number of Ad-Watch Events (internal, accepted and blocked)
Blocked: Total number of events that have been blocked by the user
Accepted: Total number of events that have been accepted by the user

Details

Processes Blocked: Total number of processes blocked
Browser Hijack Attempts Blocked: Total number of attempted browser hijacks blocked
Other Registry Events Blocked: Total number of blocked registry changes not specifically defined in the definitions file
Tracking Cookies Blocked: Total number of tracking cookies blocked
Pop-ups Blocked: Total number of pop-ups blocked
Internal Events: Initialization events, warnings and Ad-Aware specific events

Links

Export As Textfile: Exports the Ad-Watch statistics to a text file
Reset Statistics: Resets the statistics to zero

8 What is Process-Watch?

Ad-Aware SE Professional Edition comes with Process-Watch, a powerful process viewer/manager. It allows browsing, scanning, and termination of running processes (and their associated modules), as well as using installed extensions to further analyze a running process or module. Using extensions require that you first select an item in the list and then pick the extension to use from the context menu

Process-Watch shows you a snapshot of all the running processes (top) and their associated modules (bottom) at the time Process-Watch is launched. This snapshot can be refreshed at any time by clicking the "**Refresh**" button or right-click to bring up the context menu and select "**Refresh**".

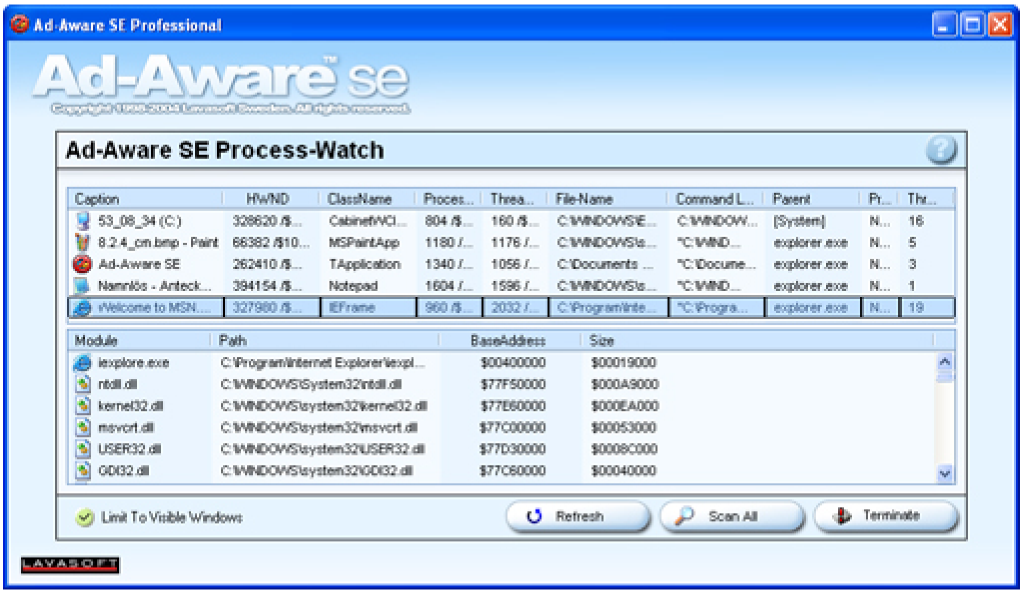
Process-Watch displays two lists with information, the upper list is the process list displaying the currently running processes in the system. The lower list is a module list showing the modules the selected process has loaded into memory

Process-Watch allows you to quickly terminate any running process or unload a module. **Be careful here!** Some processes and modules are needed by Windows or other software in order to function

You can scan the processes with Process-Watch to see if there are any known offending processes running and terminate them if necessary.

By default Process-Watch lists all processes that are connected to visible windows on the users desktop. By un-checking the "**Limit To Visible Windows**" option Process-Watch will show all currently running processes in Windows including all background processes.

8.1 The Interface


Ad-Aware SE Professional
Ad-Aware™ se
Copyright 1998-2004 Lavasoft Sweden. All rights reserved.
Ad-Aware SE Process-Watch
?
Refresh
Scan All
Terminate
LAVASOFT

Caption	HWND	ClassName	Proces...	Threa...	File-Name	Command L...	Parent	Pr...	Thr...
53_08_34 (C:)	328620 /$...	CabinetWCl...	804 /$...	160 /$...	C:\WINDOWS\E...	C:\WINDOW...	[System]	N...	16
8.2.4_cm.bmp - Paint	66382 /$10...	MSPaintApp	1180 /...	1176 /...	C:\WINDOWS\s...	"C:\WIND...	explorer.exe	N...	5
Ad-Aware SE	262410 /$...	TApplication	1340 /...	1056 /...	C:\Documents ...	"C:\Docume...	explorer.exe	N...	3
Namnlös - Anteck...	394154 /$...	Notepad	1604 /...	1596 /...	C:\WINDOWS\s...	"C:\WIND...	explorer.exe	N...	1
Welcome to MSN....	327980 /$...	IEFrame	960 /$...	2032 /...	C:\Program\Inte...	"C:\Progra...	explorer.exe	N...	19

Module	Path	BaseAddress	Size
iexplore.exe	C:\Program\Internet Explorer\iexpl...	$00400000	$00019000
ntdll.dll	C:\WINDOWS\System32\ntdll.dll	$77F50000	$000A9000
kernel32.dll	C:\WINDOWS\system32\kernel32.dll	$77E60000	$000EA000
msvcrt.dll	C:\WINDOWS\system32\msvcrt.dll	$77C00000	$00053000
USER32.dll	C:\WINDOWS\system32\USER32.dll	$77D30000	$0008C000
GDI32.dll	C:\WINDOWS\system32\GDI32.dll	$77C60000	$00040000

☑ Limit To Visible Windows

Buttons
?: Shows the quick help tips for Process-Watch
Refresh: Creates a new process snapshot and refreshes the information in the process and module window
Scan All: This will scan the executable files for all processes. Using this function deactivates the filtering. If any suspected processes are found, they will be listed in red.
Terminate: This will terminate the selected process.

Tips!
Double-clicking on any process will open the Windows properties for the process.

Double-clicking on any module will dump the selected process memory image/area and display it in a window.

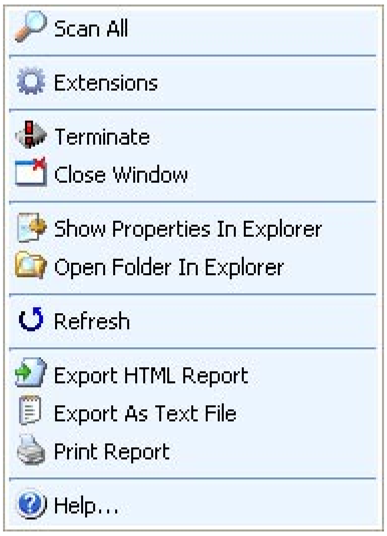
Keyboard shortcuts\functions

Cursor up\down = Navigate through the lists
F5 = Refresh (Updates the entire list)
CTRL + N = Jump to next recognized target. This only works if the list contains a recognized suspicious process
CTRL + P = Jump to previous recognized target. This only works if the list contains a recognized suspicious process
CTRL + T = Terminate currently selected process. This will work with any listed process or module

Process snapshot window

Caption: The window title. If the visibility filter is set, windows without a title and not matching a certain windows class will not be listed.
HWND: The handle assigned by Windows to the selected process
ClassName: The window class name
Process ID: The unique identifier for the process
Thread ID: The unique identifier for the main thread of the process
File-Name: The path and file name information of the file spawning the selected process
Command Line: The command line used to start the process. It includes path and file name information of the executable file and the command line arguments passed to the process as startup.
Parent: The parent process of the selected process
Priority: The base priority of threads created by this process
Threads: Number of threads created by the selected process

Right-click to open the context menu where more options are available



Process snapshot window context menu

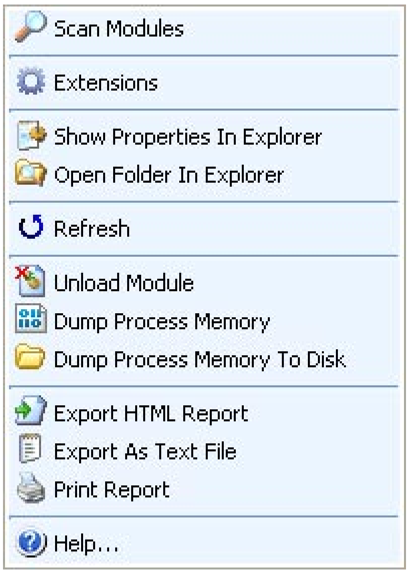
Scan all: This will scan the executable files for all processes. Using this function deactivates the filtering. If any suspected processes are found, they will be listed in red.
Extensions: Shows available extensions for further analysis of the selected process
Terminate: Terminate the selected process
Close Window: Close the selected window without terminating the process. This is useful for closing explorer.exe windows without killing the explorer.exe process.
Show Properties In Explorer: Shows file properties for the file spawning the selected process
Open Folder In Explorer: Opens the folder that contains the file spawning the selected process
Refresh: Creates a new process snapshot and refreshes the information in the process and module windows
Export HTML Report: Export the process snapshot as a HTML formatted report including the

processes listed in the process window
Export As Text Document: Export the process snapshot as a text file including the processes listed in the process window
Print Report: Print the process snapshot including the processes listed in the process window
Help: Open the Ad-Aware help file

Module snapshot window

Module: File name of the module
Path: Full path and file name of the module
Base: Base address of the module relative to the owning process
Size: The allocated memory size for the selected module

Right-click to open the context menu where more options are available



Module snapshot window context menu

Scan Modules: This will scan all modules loaded by the currently selected process. Using this function deactivates the filtering. If any suspected modules are found, they will be listed in red.
Extensions: Shows available extensions for further analysis of the selected module
Show Properties In Explorer: Displays the Windows properties for the module
Open Folder In Explorer: Opens the folder that contains the file spawning the selected module
Refresh: Creates a new process snapshot and refreshes the information in the process and module windows
Unload Module: Unload the selected module form memory
Dump Process Memory: Dump the selected process memory image/area and display it in a window
Dump Process Memory To Disk: Dump the selected process memory image/area and save it as a file
Export HTML Report: Export the module snapshot as a HTML formatted report including the modules listed in the module window
Export As Text File: Export the module snapshot as a text file including the modules listed in the module window
Print Report: Print the module snapshot including the modules listed in the module window
Help: Open the Ad-Aware help file

9 Purchasing additional solutions from Lavasoft

Please see the following for links to our purchase pages, customer care center, and payment options/information

Home user

Please visit http://www.lavasoft.de/purchase/home/*
For sales questions please contact sales@lavasoft.de**

Business Customers

Please visit http://www.lavasoft.de/purchase/business/*
For sales questions please contact corporatesales@lavasoft.de**

Customer Care Center

Visit Lavasoft's Customer Care Center*.

* You must be connected to the Internet to access this link
** Please note that this e-mail address is for sales related questions only. Technical support questions sent to this address will not be answered.

10 Support

Support Forums

Our online support forums are available 24 hours a day, 7 days a week at www.lavasoftsupport.com*. Registration is required in order to post. The registration is free and you are not required to publicly display any information about yourself. Your account registration request must be validated by the support forums administrators and may take up to 24 hours. The Administrators and Moderators at the Support Forums will answer your questions as quickly as possible but do not staff the forums 24 hours a day. Please be patient if your inquiry is not answered right away. You can also search the forums for the information you are seeking as we have a large community and a tremendous amount of available information

Knowledge Base

The Knowledge Base is an interactive tool containing technical solutions compiled by Lavasoft to help you solve a variety of technical support or customer service information issues you might have regarding the configuration and usage of all the products included in the Lavasoft family
Search the Knowledge Base*

Threat Assessment Chart - TAC

Information about the items detected by Ad-Aware can be found in the TAC database.
Search the TAC database*

Help Online

Lavasoft's support website contains documentation and information about our products. At www.lavasofthelp.com* you will find Frequently Asked Questions, How To Guides, Knowledge Base, online demos and other useful information.

Lavasoft Support

Through your purchase you are also eligible for support through our customer center. To contact Lavasoft's support department please fill out this support form* on our website.

In addition to the on-line support for our registered customers, we also provide POC (Point Of Contact) support to our large corporate and Enterprise customers. SLAs (Service Level Agreements) are available upon request

* You must be connected to the Internet to access this link

10.1 Support Forums

Our online support forums are available 24 hours a day, 7 days a week at www.lavasoftsupport.com*. Registration is required in order to post. The registration is free and you are not required to publicly display any information about yourself. Your account registration request must be validated by the support forums administrators and may take up to 24 hours. The Administrators and Moderators at the Support Forums will answer your questions as quickly as possible but do not staff the forums 24 hours a day. Please be patient if your inquiry is not answered right away. You can also search the forums for the information you are seeking as we have a large community and a tremendous amount of available information

* You must be connected to the Internet to access this link

10.1.1 Support Forums FAQ

How to register at the Lavasoft Support Forums

1. Go to the forums at www.lavasoftsupport.com*.
2. Click on "**Register**".

3. Complete the form.
4. Read the Terms of Service, acceptance is required.
5. Submit the registration.
6. You will receive a validation email within 24 hours.

How to start a topic at the Lavasoft Support Forums

1. Log in using the username and password that you have chosen.
2. Click on the forum title that matches the version of Ad-Aware SE that you use.
3. On the page that opens, click on the button that say's "**New Topic**".
4. On the page that opens, type your message in the window.
5. When finished, click on the "**Post New Topic**" button.
6. You can also edit your post afterwards by clicking the "**Edit**" button.

Posting logfiles

When posting a question at the Lavasoft Support Forums it is likely that you will be asked to post a log file. Before the Lavasoft Personnel at the Support Forums can help with a removal, they must first see a log file of the scan. The log file shows them the pertinent information needed to ensure that Ad-Aware and the definitions file are up to date. The log file lists the processes that are running in the computer at the time of the scan, the objects that were detected during the scan, and other environmental information.

Before posting your logfile

Before you post your log file you should make sure your copy of Ad-Aware is up to date. Start by checking the version number, in the lower right corner of the Ad-Aware program window. Then run WebUpdate to make sure you are using the latest definition file. If a new file is available, download it and run a new scan.

How to post your logfile

1. Scan with Ad-Aware,
2. When the scan is complete click the "**Show logfile**" button
3. Right click in the window and choose "**Select all**"
4. Right click again and choose "**Copy to clipboard**"
5. Go to the support forums and start a new post.
6. Right click in the text field and select "**Paste**"

How to recover a lost password

1. Go to www.lavasoftsupport.com* and click on "**Log in**" at the top left.
2. In the page that appears you will find a link, "**I've forgotten my password! Click here!**"
3. Follow the directions on the page that appears.
4. Click "**Proceed**".
5. An email will be sent to the address you registered with.
6. In the e-mail you will be given a link* that will take you to a webpage that you can enter a new password.
7. Click on "**Proceed**".

You will now be able to login.

* You must be connected to the Internet to access this link

10.2 Knowledge Base

The Lavasoft Knowledge Base service is offered at no charge to all of our customers and partners worldwide. The Knowledge Base is an interactive tool containing technical solutions compiled by Lavasoft to help you solve a variety of technical support or customer service information issues you might have regarding the configuration and usage of all the products included in the Lavasoft family

In addition the Knowledge Base offers you product manuals, links to downloadable software files, and patches required to handle technical issues.
Search the Knowledge Base*

* You must be connected to the Internet to access this link

10.3 Threat Assessment Chart - TAC

All items detected by Ad-Aware are qualified using a Threat Assessment Chart (TAC) prior to inclusion. The system is based on a total of 10 points, 1 being the least and 10 being the most threatening and/or problematic. Behavior and intent weigh more heavily towards becoming a legitimate detection than do the technical aspects. Please note that applications that are difficult to remove and cause system instability due to poor coding and DO NOT contain any further violations as described below ARE NOT considered for inclusion in the Ad-Aware database.

Information about the items Ad-Aware detects can be found in the TAC database.
Search the TAC database*

* You must be connected to the Internet to access this link

Here are the criteria we use to determine if something should be added to our database:

Removal

Given one point.

Determining factors:
- Provides no uninstaller at all or non-functional application uninstaller.
- Lacks clear evidence of intention. In other words, there is no available evidence to suspect the application's developer of intentionally making his/her software difficult to uninstall other than having a poorly coded or buggy uninstaller.

Integration

Can cause system instability and is worth two points.

Determining factors:
- This category refers to the effect a given database candidate has on a user's system.

Distribution

Unsolicited Install and is given two points

Determining factors:
- Intentionally hidden (stealth) install and/or clear evidence of Intention. The application is designed with the clear intention of either making it difficult or impossible to remove using normal removal procedures.
- Bundled install that is undisclosed. This is different from the previous determining factor, but there was no notice given to the user pre-install and/or the host application's EULA (End User License Agreement) attempts to hide the application's inclusion as a condition of the host application's install and/or use.
- Program does not disclose info in EULA, has a confusing EULA, or a hidden EULA listing what is done with collected information.

Behavior

Malware is given three points automatically regardless of the stated behaviors listed below. All other intentional behaviors are given three points.

Determining factors:
- Virus / Trojan Horse.

- Connects to perform or aid in a DDoS (Dedicated Denial of Service) attack.
- Program masks as doing one thing, but does another.
- Use or creation of Tracking Cookies.
- Changes browsing results (browser hijack/redirect, replace text/graphics, opens random websites).
- Operates in stealth (Runs hidden from the user).
- Opens web sites not initiated by the user/unsolicited Popups and/or requests to join a different site.
- Auto-updates without user permission and/or knowledge.
- Dials an unprompted or unauthorized Internet connection.
- Opens or Exploits a System Vulnerability.

Privacy

Privacy Violations are worth two points.

Determining factors:

- Connects to a remote system with or without the user's awareness to transmit usage statistics and/or personally identifiable information.
- Connects to a remote system without the user's awareness to transmit/receive information.
- Tracks the user's surfing habits.

Index

- / -

/? 46
/ads 46
/custom 46
/full 46
/help 46
/paths:"%pathsfile%" 46
/sdump:"%destinationfile%" 46
/smart 46

- + -

+archives 46
+auto 46
+cskip 46
+delay 46
+diskonly 46
+log:"%destination%" 46
+mru 46
+nice+/-n 46
+nodefnotice 46
+noset 46
+nowrite 46
+prefs:"%file%" 46
+procnuke 46
+ref:"%file%" 46
+remove:n 46
+retv 46
+safeload 46
+silent 46
+update 46

- A -

Activity 58
Ad-Aware configuration 31
Ad-Aware Statistics 29, 53
Add New Rule 60
Add-on 27, 28, 29, 53
Add-ons 27, 28, 29, 53
ADS 3
Advanced Automation 51
Advanced Options 34
Ad-Watch 39, 55
Ad-Watch configuration 56
Ad-Watch Event Log 55
Ad-Watch Options 58
Ad-Watch rules 59
Ad-Watch Statistics 63
Ad-Watch Tools & Preferences 56
Alternate Data Streams 3, 34

- - -

-archives 46
Automated 51
Automated scans 51
Automatic Cleaning 50
Automatic Quarantine 50
Automatic Scans 50
Automatic Updating 35
Automatic WebUpdate 45, 50
automation 7
Available command line parameters 46

- B -

Block URL 62
Blocking Options 58

- C -

Change language 48
Changing skin 48
Cleaning Engine 39
Code Sequence Identification 3
command line 46
Command Line Parameters 45, 46
configuration 31, 32, 33, 34, 35, 37, 38, 39
Critical 16
Critical Objects 16
CSI 3
Customer Care Center 67

- D -

Default IE Pages 37
Default Settings 37
definition file 45
Definitions 32
download 6
Download add-on 53
Drives & Folders 33

- E -

Event Filtering 59
Event-History 58
expert settings 39
Extension 27, 28
Extensions 27, 28, 53

- F -

Filter 61
first scan 50

- G -

General Options 32

- H -

Help Online 68

- I -

Ignore 22, 49
Ignore list 22, 49
Install 6
Install add-on 53
Interface Settings 38

- K -

Knowledge Base 68, 69

- L -

Language 48
Language File 38, 48
Language Pack 48
Lavasoft Support 68
Logfile Detail Level 34
Logfiles 39
Logging & Maintenance 58

- M -

Main menu 10
Manual Update 45
Memory & Registry 33
Misc Settings 39
Module snapshot 64

- - -

-mru 46

- N -

Negligible 19
Negligible Objects 19
Network Updating 45

- O -

Operating Systems 4
options 31, 32, 33, 34, 35, 37, 38, 39

- P -

Performing System Scan 13
Performing WebUpdate 25
Play Wavefile 38
Pop-ups 62
Preparing System Scan 11
process manager 64
Process snapshot 64
process viewer 64
Process-Watch 64
Proxy 26
purchase 67
Purchasing 67

- Q -

Quarantine 24, 48
quarantine archive 48
Quarantine Log 24
Quarantine Manager 24, 48
quarantine objects 48
Quarantined Objects 24
Quick launch 10
Quick Tip 10

- R -

Real Time Accuracy 58
real time monitor 55
real time protection 55
RegHance Executable 37
Reset Ad-Aware Settings 37
Restore quarantined objects 48
Rule Editor 59
Run add-on 53
Run extension 53
Run tool 53

- S -

Safety Settings 32, 39
scan 7
Scan Complete 14
Scan Log 21
Scan Settings 33
Scan Summary 15
Scanning Engine 39
Scanning Results 15, 16, 19, 21
Select Skin 38
Setting up 50
Setting up Ad-Aware 50
Settings 31, 32, 33, 34, 35, 37, 38, 39
Shell Integration 34
Simple Startup Scan 51
sites.txt 62
Startup Action 35
Startup Scan mode 35
Startup Settings 35
Statistics 27, 29, 53, 63
Status screen 11
Support 68, 69, 70
Support Forums 68
System Requirements 4

- T -

TAC 68, 70
TAC database 70
Threat Assessment Chart 68, 70
Tool 27
Tools 27, 53
Tools & Preferences 56
Tracking Cookie Blocking 3
Tweak Settings 39

- U -

Uninstall 9
uninstall add-on 54
Uninstaller 9
Update the definition file 45
User Interface 39

- W -

WebUpdate 25, 26, 27, 45
WebUpdate Configuration 26
WebUpdate Settings 39
Windows Task Scheduler 51
Virus 52
Virus warnings 52