

Ad-Aware Tutorial

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 "**aawsepersonal.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 Personal.

4. Destination Location

Click "**Next**" to accept the default location or use "**Browse**" to specify where you want Ad-Aware SE Personal 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 Personal 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**".

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.

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.

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 antispymware 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 antispysware 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.

Performing System Scan

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

Scan Complete

When a scan is completed the [Performing System Scan](#) screen will change name to "**Scan Complete**".

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

Scan Summary

Shows a summary of the Scanning Results.

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.

Critical Objects

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

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.

Quarantined Objects

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

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 two 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.)

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 Personal\
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](#).

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

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

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.

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.

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