

# Virus & Spy Protection

For Virus Protection download Free AVG Anti-Virus 7.5  
[www.free.grisoft.com/](http://www.free.grisoft.com/)

Below is a screen shot of Free AVG Anti-Virus 7.5. After installation you will be prompted to go through a series of checks, after completing all of those steps in the future you must only click on the button to the left of “Scan Computer.” The software itself will automatically update itself when needed after the computer is started.



When you feel it is needed perform the system scan by clicking on “Scan Computer.” The software will auto scan any new things installed and downloaded, but it is still a good idea to perform this task every 2-3 months and right after installation.

## Spybot Search and Destroy

Before you begin, download Spybot S&D from <http://www.download.com/>. On the download.com website search for Spybot, it will be the first selection with over 80 million downloads.

1) The first time you start Spybot-S&D, it will display a *Wizard*, a small window helping you through the first steps. It gives you the possibility to add or remove the icons you have or haven't created during install, for example. Let's just say you want them and proceed to the next page.

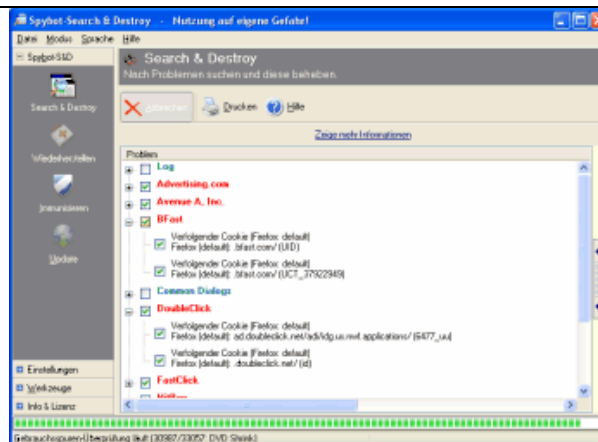
If you are using a proxy in Internet Explorer, Spybot-S&D will show you this proxy and a button will give you the opportunity to use it for Spybot-S&D, too. If the text field is blank, you don't need to do it, but in most cases this will show an internet address, and you should import this proxy setting.

The next page deals with updates. It is very important to keep up-to-date. Using the two buttons this page offers will do the updates for you. The last page of the wizard will ask you to read the help file. The help file is always a good resource if you are unsure what to do, so please do at least read the first pages of it.



2) After the tutorial has finished, you may find yourself on the *Settings* or *Update* page. As the default settings are ok right now, and you've already updated, let's ignore them for now and do the first scan.

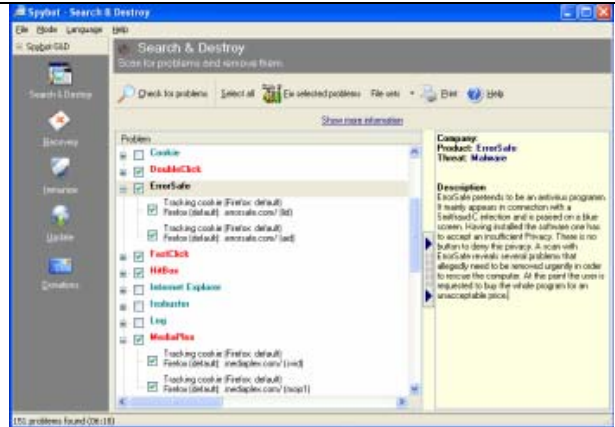
The left side of the program has a navigation bar that can lead you to all functions of the program. The first section there (the top-most button) is labeled *Spybot-S&D* and leads you to the main page. Right now, you will see only an empty list and a toolbar at the bottom. The first button in this toolbar is named *Check for problems* - that is the button you've got to press to start the scanning. Lean back and watch the scan progress.



3) At this point, you could just jump to point 7, and remove the results. Instead we recommend that you first have a look at what all the stuff is that Spybot-S&D detected. The first thing you should know is to distinguish between the red entries, which represent spyware and similar threats, and the green entries, which are usage tracks.

For the usage tracks (I hope you have followed that link to read what they are), removal is non-critical, but depends on your personal preferences.

Ignoring the usage tracks for now, you should have a look at the red entries which represent the real threats. While you of course can trust us that we have chosen the targets using strict criteria, you can check for yourself if you click on each product and read the product information that will be shown in a pop-up window.



4) All problems displayed in red are regarded as real threats and should be dealt with. But while you read the product description, you may still decide to keep a threat, or just a usage track. Maybe you don't want your list of most recently used Word documents removed? At this point you have three options.

- You could decide on ignoring all usage tracks. In that case you could open the *File sets* page on the *Settings* section of the program, and disable the *Usage tracks* entries.
- Or if you want to just keep all tracks from a specific product, just right-click a product in the results list.
- Finally, if you want to keep just one file, that is possible the same way.

5) So now you should know about everything you've found. It's time to use the *Fix selected problems* button.

Once you start thinking about removing the usage tracks, too, you may think that ticking all the green entries is hard work. This is for a simple reason - to force you, the newbie - to look at the results. Once you know what you are dealing with, there is a hidden *Select all* button available for you.

# Ad-Aware SE

## Introduction

If you suspect that you have spyware installed on your computer, then an excellent tool to remove them is Ad-Aware SE. Follow the instructions below to learn how to use Ad-Aware SE to remove these programs from your computer. Word of warning, though, spyware can sometimes be integrated tightly into software that you use, and if you remove the spyware, that software may not function correctly. So be careful as to what you remove.

If you would like to learn more about spyware and Browser Hijackers you can click here:

Understanding spyware and Browser Hijackers

## How to use Ad-Aware SE

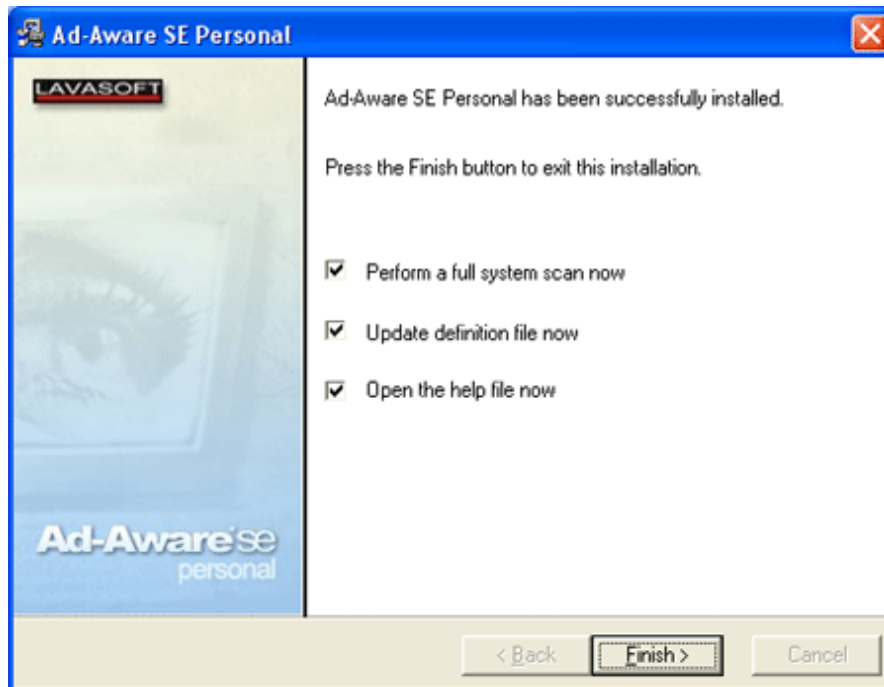
### **Step 1: Download Ad-Aware SE**

The first step for Spyware/Hijacker removal is to download and install Ad-Aware SE from the link below. After it is installed, continue with the following steps.

**Note: There may at times be programs listed above in the Google ads that seem similar to the programs we recommend. These are usually not the same program. Bleeping Computer has no real say as to what appears there and can not vouch for any of those programs. Please use only the programs directed to you by us in the forums or via these tutorials.**

Please download Ad-Aware SE from <http://www.download.com>, simply search for Ad-Aware and proceed.

Download this program to a location on your hard drive that you will be able to find later. When the download is finished navigate to that location using Windows Explorer or My Computer, and double click on the file name. The file name generally starts with aawse.exe. For example for the current version of Ad-Aware SE Personal, the filename is aawsepersonal.exe. Follow the defaults settings when presented with options and after the program finishes installing you will be presented with a screen similar to the one below:



**Figure 1: Options after finished installed**

Uncheck all options as we will have you manually do each of these steps in the next section. Then press the **Finish** button.

**Step 2: Start Ad-aware SE**

On your desktop, double click on the icon for Ad-Aware SE.

The program will open and it will appear as in Figure 2 below.

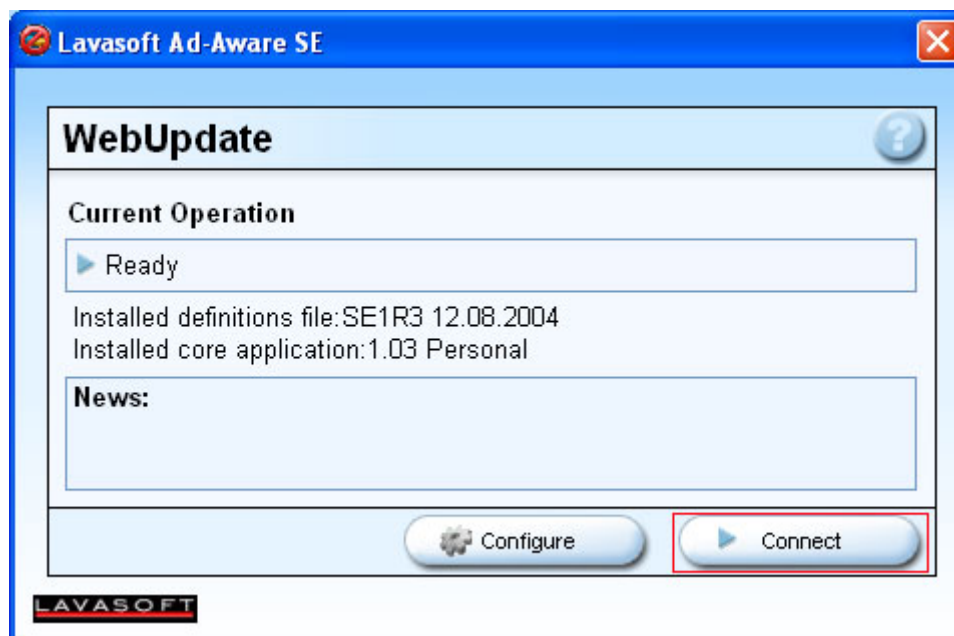


**Figure 2. Ad-Aware SE Starting/Status Screen**

This is the main startup/status screen for Ad-Aware SE. Each section that is important for its use has been boxed off with a different color. The red box around the Scan Now button is used when you want to scan your computer for Spyware/Hijackers. The blue box lets you get into the options screen for Ad-aware SE. The purple box is where you would click to see what Spyware/Hijackers have been quarantined. The yellow box is used to update the malware database that the program knows how to clean.

### Step 3. Updating Ad-aware

The first step you should do is update Ad-Aware SE so it is using the latest Spyware/Hijacker definitions. This will enable the software to recognize as much of these types of programs that it can. You should click on the WebUpdate button highlighted, in the previous image, in yellow to start the update process. When you start the process you should see an image similar to Figure 3 below.



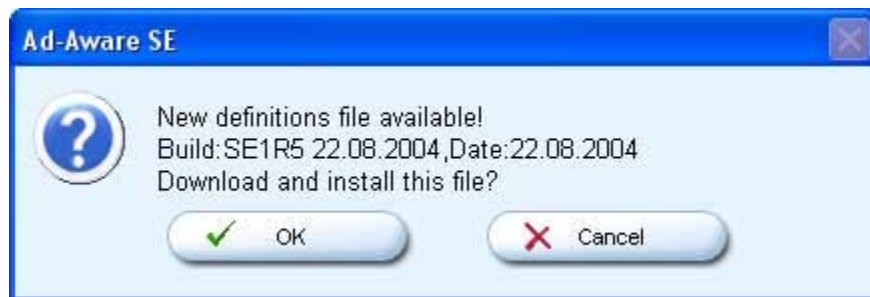
**Figure 3. Starting WebUpdate**

Now press on the connect button, designated by the red box in Figure 3, and it will check for any new updates. If no new updates are to be found you will see something like Figure 4 below. You should press OK and proceed to Step 4.



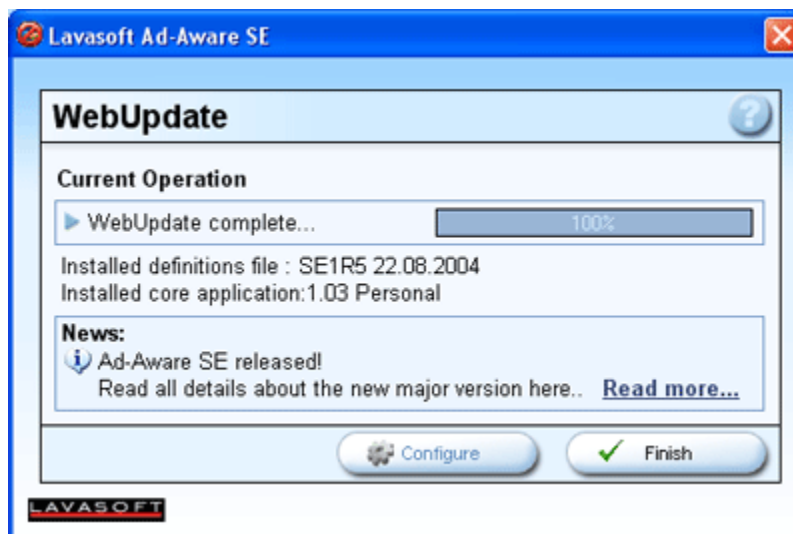
**Figure 4. No Update Found**

If an update is found you will see something like in Figure 5 below:



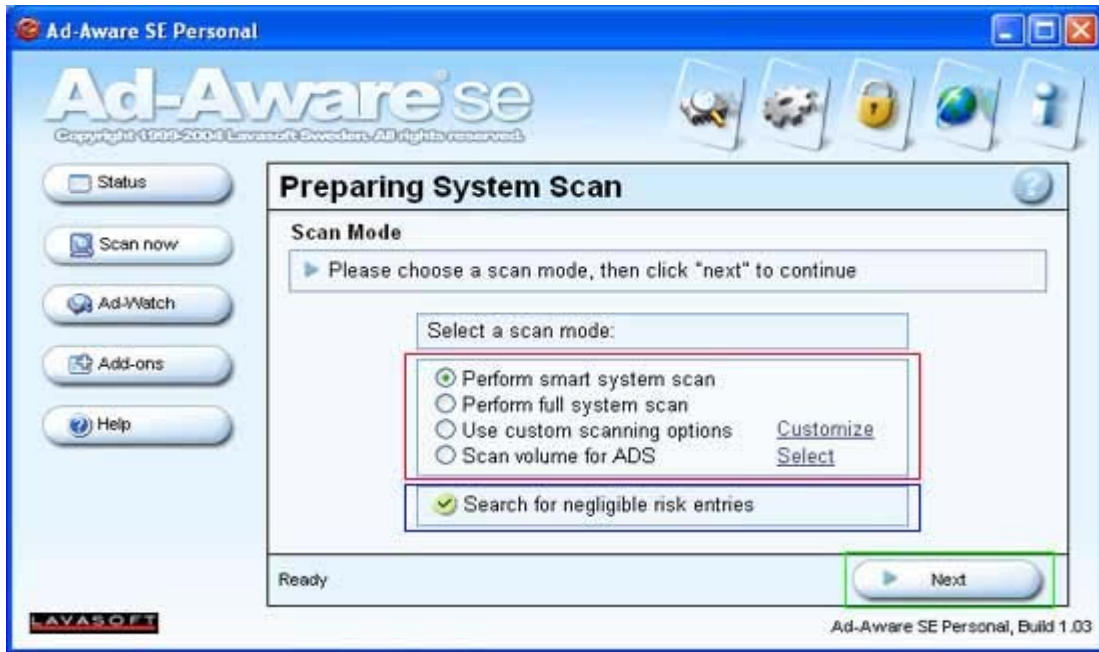
**Figure 5. Update Found**

You should click once on the OK button and let it download the update. When it is done downloading the update you will be presented with a screen similar to Figure 6 below.



**Figure 6. Updating has Finished**

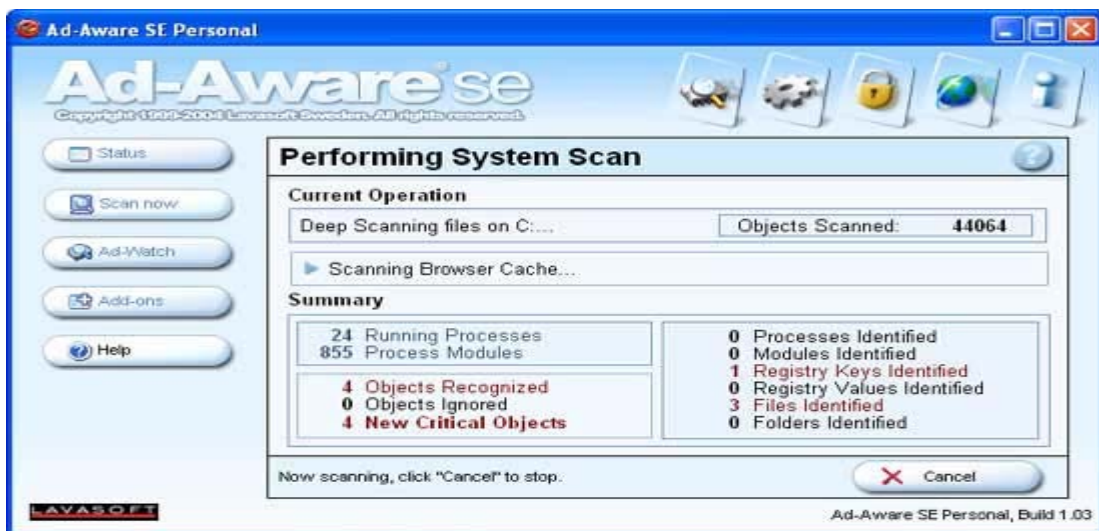
You can now click on the Finish button. When you do that you will be presented with the Status/Startup screen as shown in Figure 2. Next, click on Start in the bottom right corner which will bring you to the preparation screen as show in Figure 7 below.



**Figure 7. System Scan Preparation**

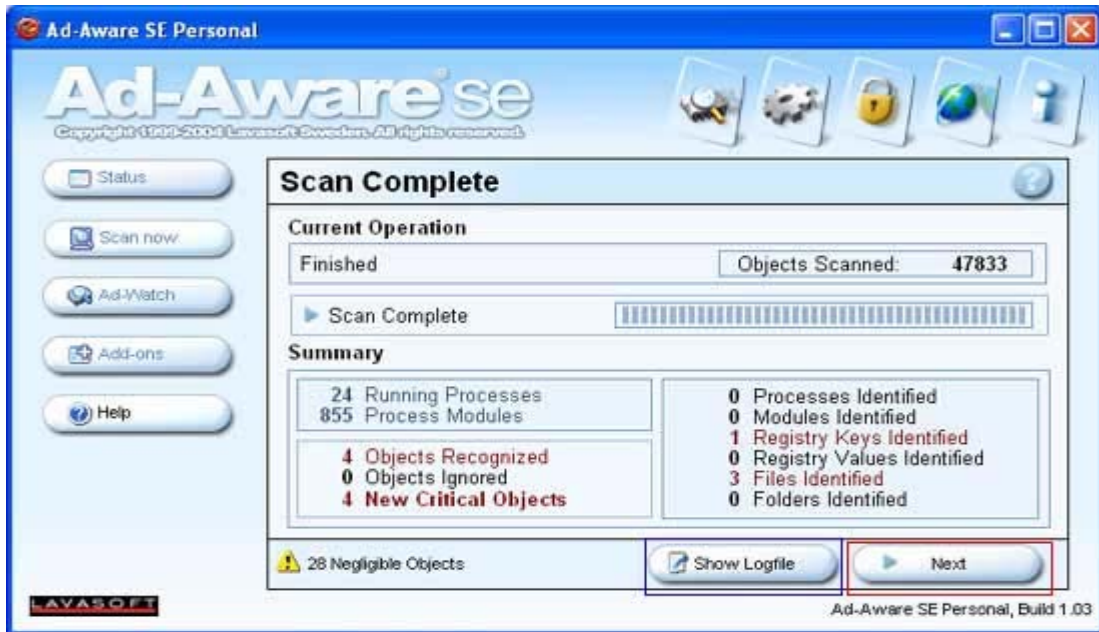
Make sure you change the scan mode, designated by the red box in the figure above, to **Perform full system scan**. Then uncheck the **Search for negligible risk entries**.

**Step 5: Start the Actual Scan** Now click on the Next button to have Ad-Aware SE start scanning your system. Ad-Aware SE will start scanning your system for Spyware and Hijackers. This could take a while, so you may want to do something else and come back and check on it occasionally. The screen will look similar to Figure 8 below.



**Figure 8: Scanning your computer**

Ad-Aware SE will scan various portions of your computer's configuration, file system, and memory for traces of known malware. As it finds infections, it will update the status of the scan with the amount of items it has found and what it is currently scanning. When it is finished scanning you will be presented with a screen similar to Figure 9 below.



**Figure 9. Finished with the Scan**

This computer has relatively few infections as you can see by the fact that it found only 4 items. If you want to copy the contents of the scan log, you can click on the **Show Logfile** button, designated by the blue box in the figure above, to open the log file and copy and paste it into another program. To finish the clean up you should now click on the **Next** button designated by the red box in Figure 9. You will then be presented with a screen that shows all the objects found that are flagged as Spyware or Hijackers as shown in Figure 10 below.



## Figure 10: Scan Results

At this point you should either right click on the screen and choose the **Select All Objects** option or individually put a checkmark in each objects checkbox, designated by the area surrounded by the red box in Figure 10, that you would like quarantined. When all the objects that you would like quarantined are checked, you should click on the **Next** button. Ad-Aware SE will now present you with a confirmation box as to whether or not you would like to remove the objects you have just selected. If you would like to do so, press the **OK** button, otherwise press the **Cancel** button to go back to the selection screen shown in Figure 10. If you press the **OK** button, Ad-Aware SE will move all the selected items into the quarantine.

When it is done putting all the checked items into quarantine, you will be presented with the Startup/Status Screen again as shown in Figure 11.

### Step 5: Cleaning up the Quarantine

With the moving of the select objects to the quarantine now completed you will be presented with a screen like Figure 11 below. As was said before, when you fix items with Ad-Aware SE it does not automatically delete them, but adds them to a quarantine file that takes up hard drive space. Therefore it is not a bad idea to get rid of them. Before you do so, though, it is good to use your computer for some time to make sure any of the items you have quarantined did not break functionality of any programs that you need to use. If you find that it has caused no problems, then you should continue.



Figure 11. Status Screen

As you can see you now have all of the items you checked off in your quarantine. To access this quarantine you should click on the link that says "Open Quarantine List". This will present you with an image like Figure 12 below.



**Figure 12. Quarantine Management**

At this point you should select the quarantine file that you would like to delete and press the delete key. The quarantine file is now deleted off your hard drive. When you are done deleting your quarantine files, you can exit the program.