

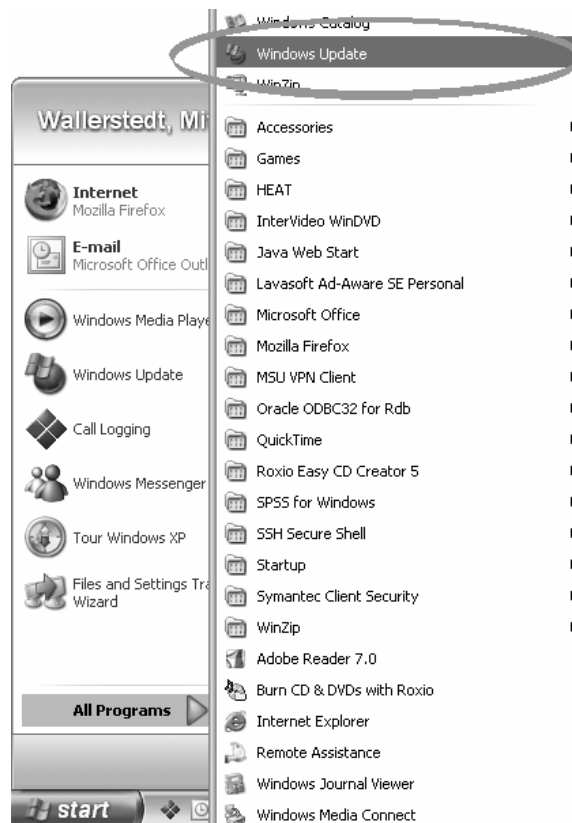
How to Keep your Windows XP PC Running Smoothly

Having problems with a slow computer? Wonder how to keep your machine running smoothly? This class will provide participants with the basic knowledge necessary to protect their Windows PCs from the most common security threats and resource thieves. Topics will include how to run Windows Updates, how to use malware removal utilities, and how to use and understand antivirus software.

Windows Updates

Manual Installation

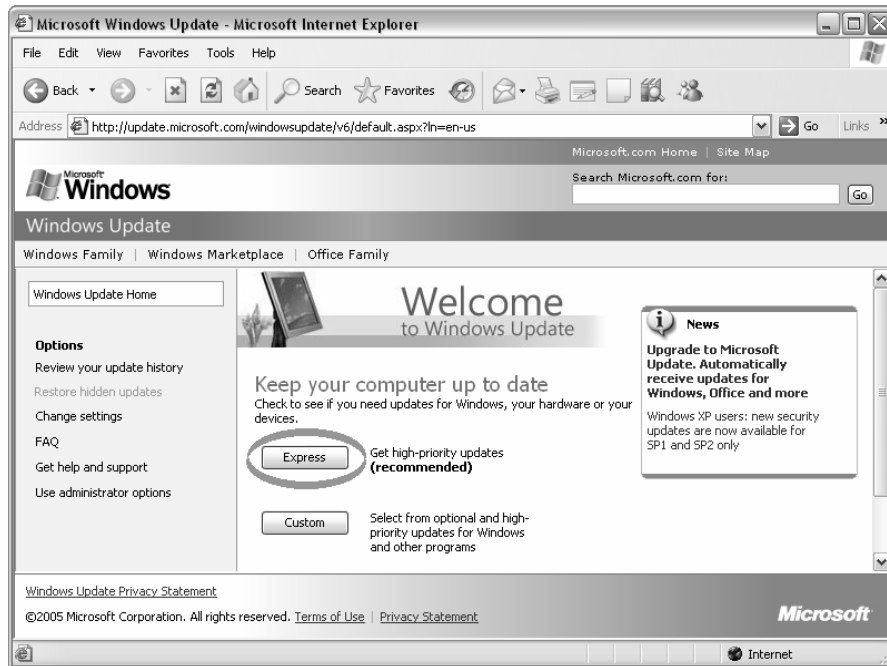
1. Click the “Start” button.
2. Move the mouse cursor over “All Programs”.
3. Select “Windows Update” from the program list.



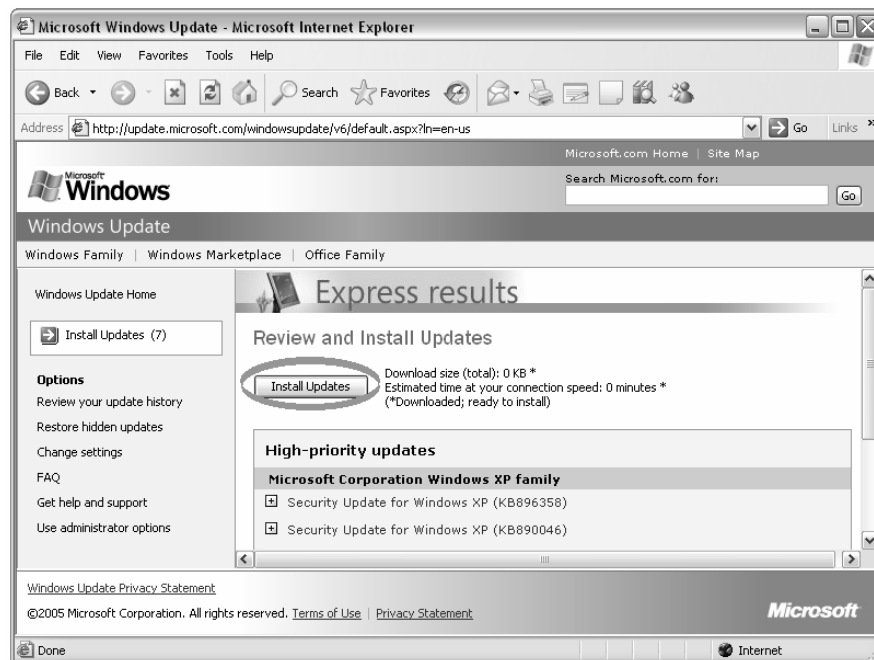
4. If prompted to, click on the “Install” button to install the Windows Update software. After the new page loads, select the “Install Now” button.

Express Install

1. Click on the “Express” button.



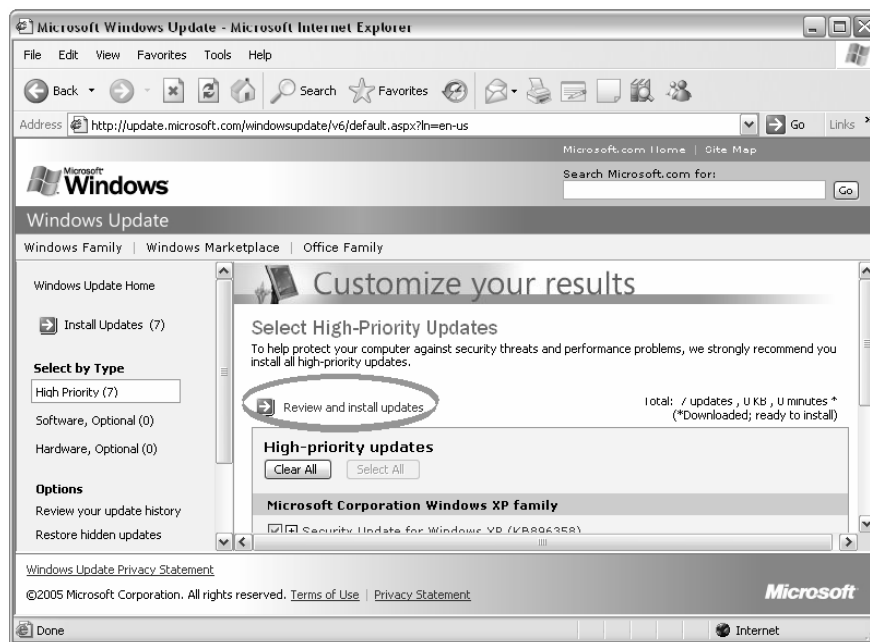
2. After a few seconds, a list of high-priority updates will be displayed. If none are found, close Internet Explorer. If updates are available, select the “Install Updates” button.



3. When the installation of the updates have completed, close Internet Explorer.

Custom Install

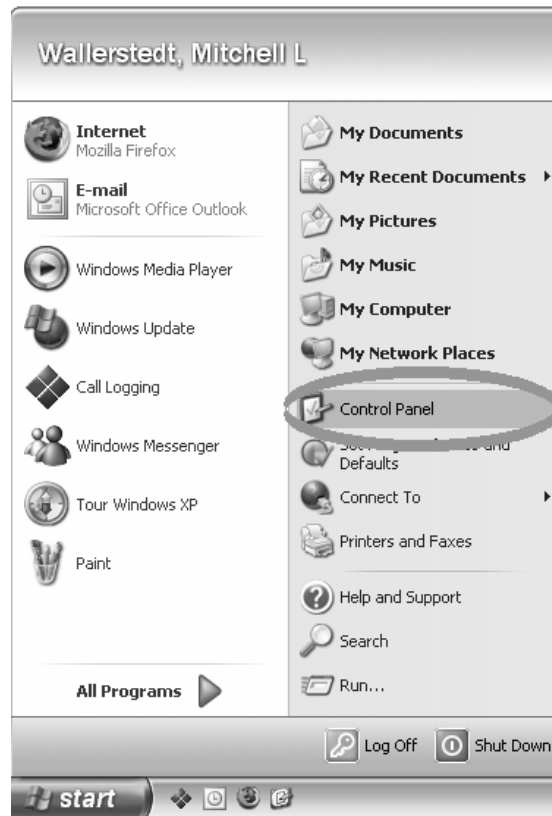
1. Click on the “Custom” button.
2. After a few seconds, a list of high-priority updates will be displayed. Also, along the left side of the window there will be a list of optional updates you may install.
3. Select “Software, Optional” to review available updates and click on the check box next to the option to mark it for installation.
4. Select “Hardware, Optional” and repeat the process from step 3.
5. Click on “Review and install updates” to view selected updates. Click on the “Install Updates” button to start the installation process.



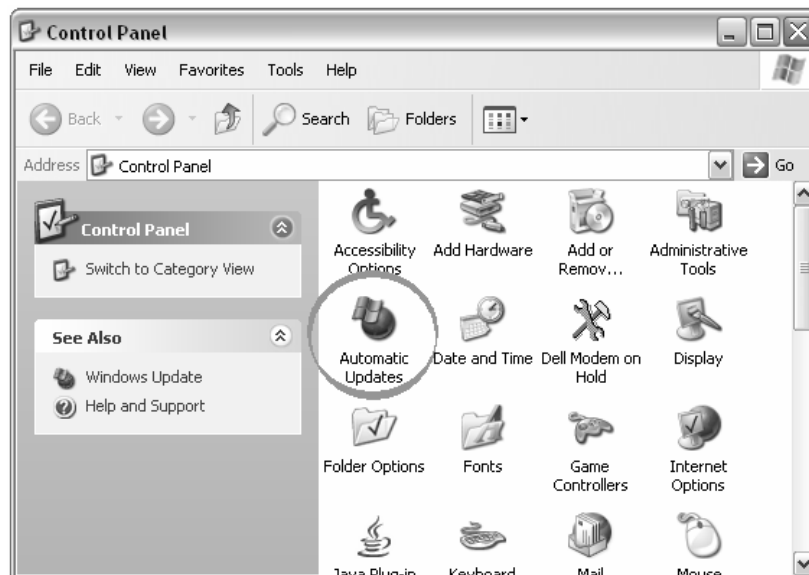
6. When the installation of the updates have completed, close Internet Explorer.

Automatic Installation

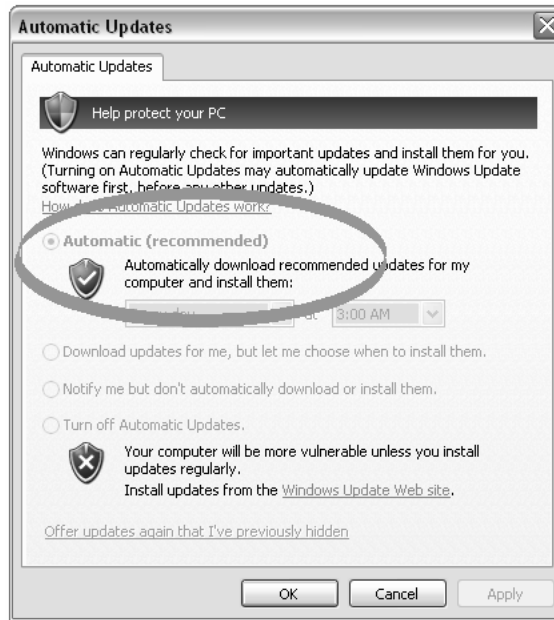
1. Click the “Start” button.
2. Select the “Control Panel” option from the Start menu.



3. Double-click the “Automatic Updates” icon.



4. Select the appropriate update option (Automatic is recommended) and click the “OK” button.



5. Close the Control Panel window.

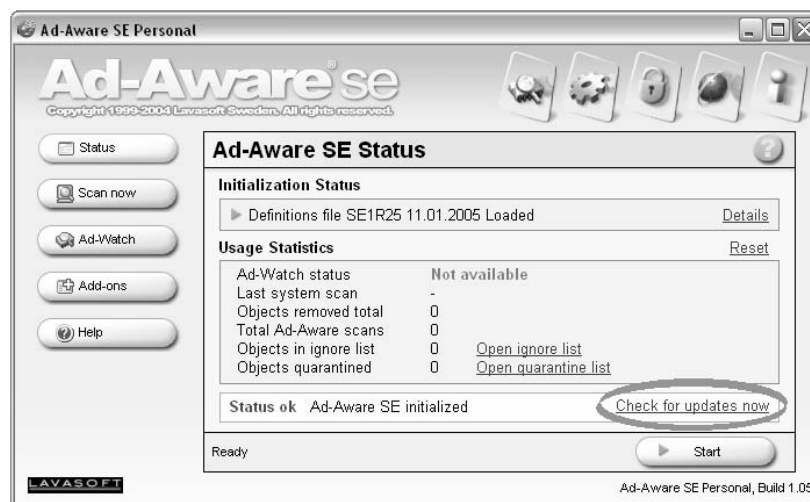
Malware Removal Utilities

Ad-Aware

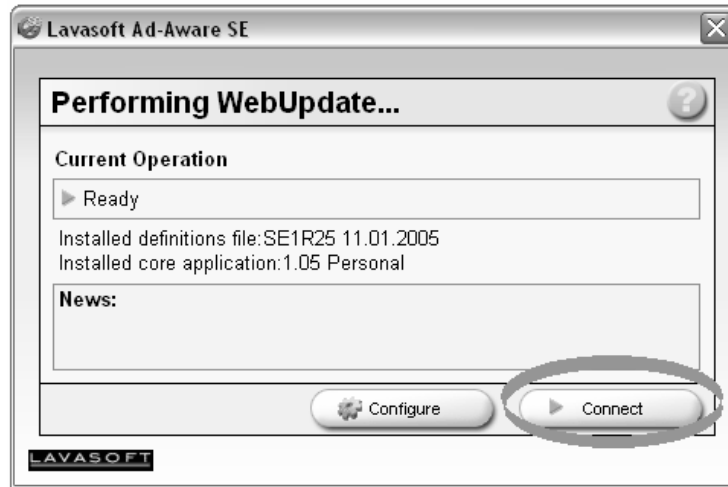
To begin, open “Ad-Aware SE Personal” from the programs list in the Start menu. If prompted to update the definitions, select “OK” and start from Step 2 under the Updates heading below.

Updates

1. Select the “Check for updates now” link.



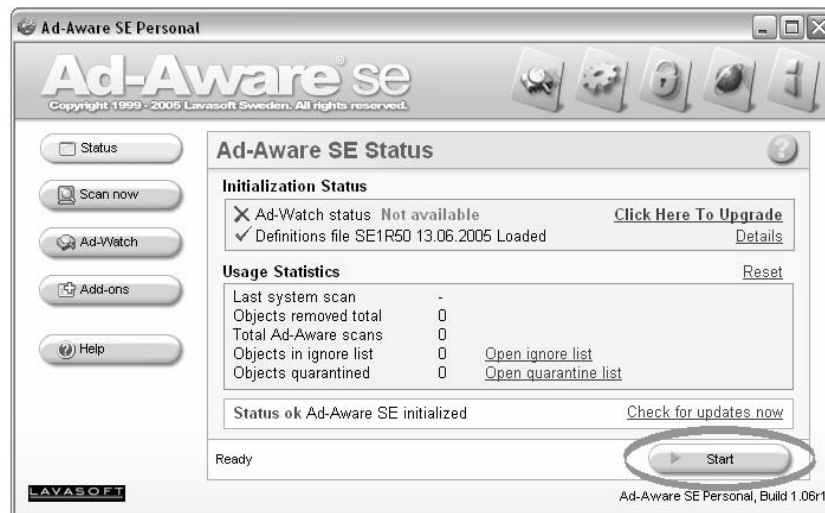
2. Click on the “Connect” button.



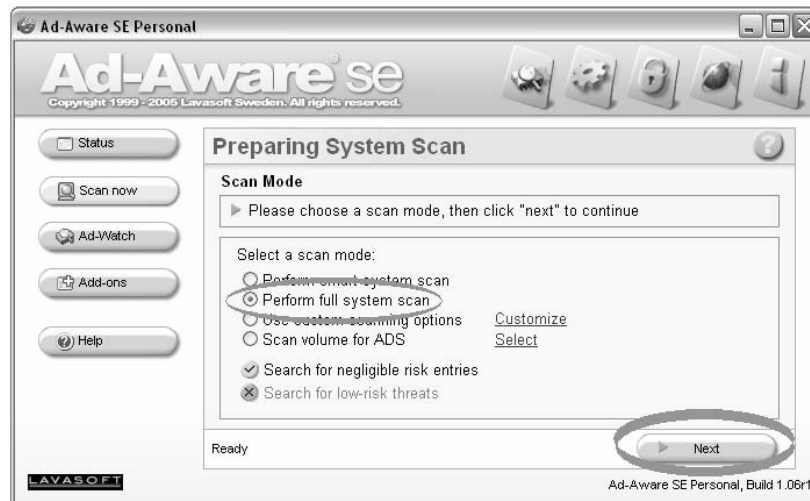
3. Select “OK” when prompted to install the updates found. Select “Finish” after installation is completed.

Usage

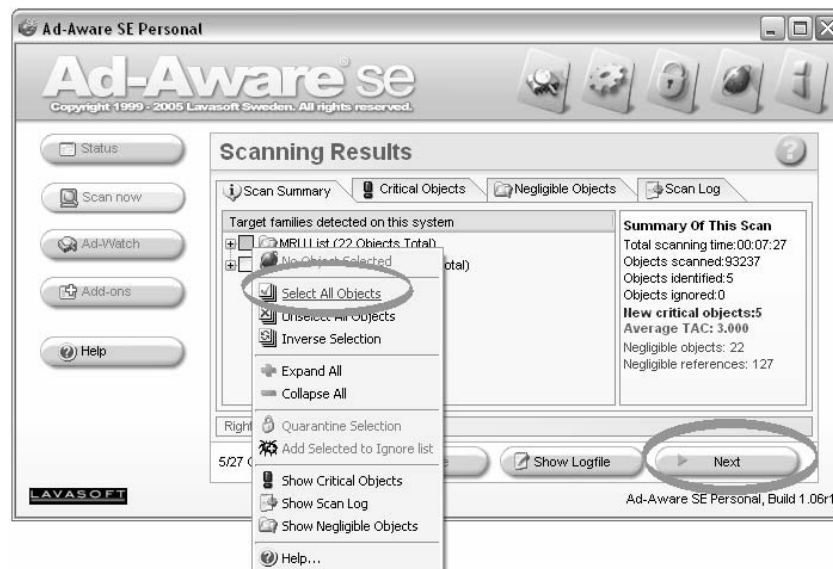
1. Click on the “Start” button.



2. Make sure that the “Perform full system scan” option is selected, then click on the “Next” button.



3. Ad-Aware will begin scanning for known threats. This will several minutes. After it has completed, select the “Next” button.
4. Under the Scan Summary tab right click on a check box next to a found threat and right click. In the popup menu choose the “Select All Objects” option and all the threats will be checked. Select the “Next” button. When prompted as to whether or not to remove these items click “OK”.



5. After the threats have been removed, Ad-Aware will return to the startup screen. You may be prompted to allow Ad-Aware to run at the system startup at this point. If so, select “OK” and Ad-Aware will run another scan next time you start your PC in order to remove additional threats. If you are not

prompted to do this startup scan then the process is complete and you can close Ad-Aware.

Spybot Search & Destroy

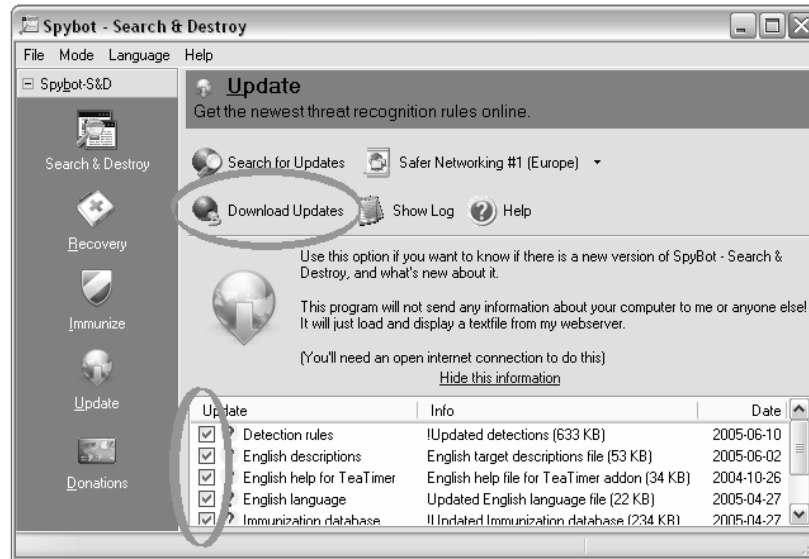
To begin, select “Spybot – Search & Destroy” from the programs list in the Start menu. The first time that Spybot S&D is opened after it is installed, a brief setup process will run. This will only run the first time; Spybot S&D will open to the regular startup screen from this point on.

Updates

1. Click on the “Search for Updates” button. After a couple of seconds, a list of available updates will be displayed.



2. Select available updates then click the “Download Updates” button. This installation will take a few seconds. When it is complete, Spybot S&D may automatically restart.

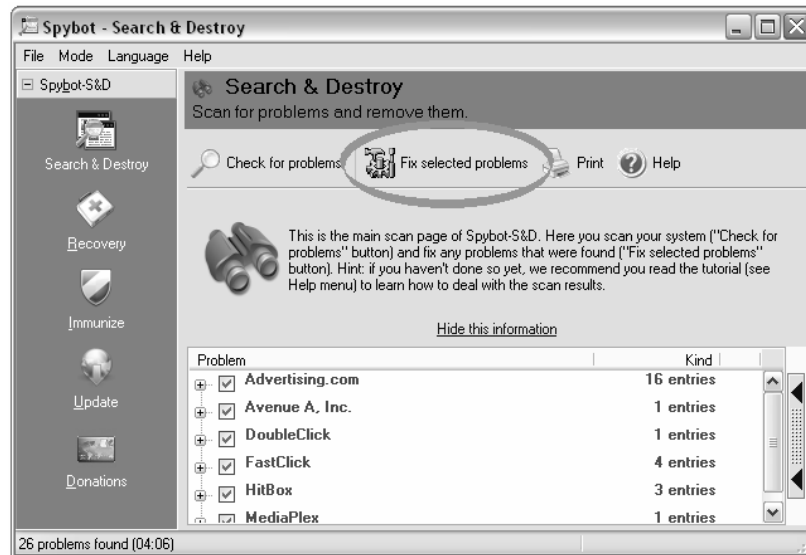


Usage

1. Click the “Check for problems” button (If you are trying to initiate a scan after installing updates, you will need to first select the “Search & Destroy” icon on the left side of the window). This will start the threat scan, which will take several minutes to complete.



2. When the scan has completed, scroll through the list of items found to make sure that all threats have been selected for removal. Click on the “Fix selected problems” button.



3. Select the “Yes” button when asked if you are certain that you would like to remove selected items and “OK” when notified that the threats have been deleted. At this point you may be asked if Spybot S&D can run at the next startup to remove items that could not be fixed initially. If asked, select “Yes” and Spybot S&D will automatically scan at the next system boot.
4. When the selected threats have been removed the process is complete. Close Spybot S&D.

Microsoft AntiSpyware

Begin by opening MS AntiSpyware from the program list in the Start menu. The first time you launch the program a setup process will automatically startup. Complete this process by following the instructions (and selecting the recommended options).

Updates

Manual Installation

1. Select the “Spyware Definitions” option from the main startup screen. The update server will be contacted and any available updates will be downloaded.



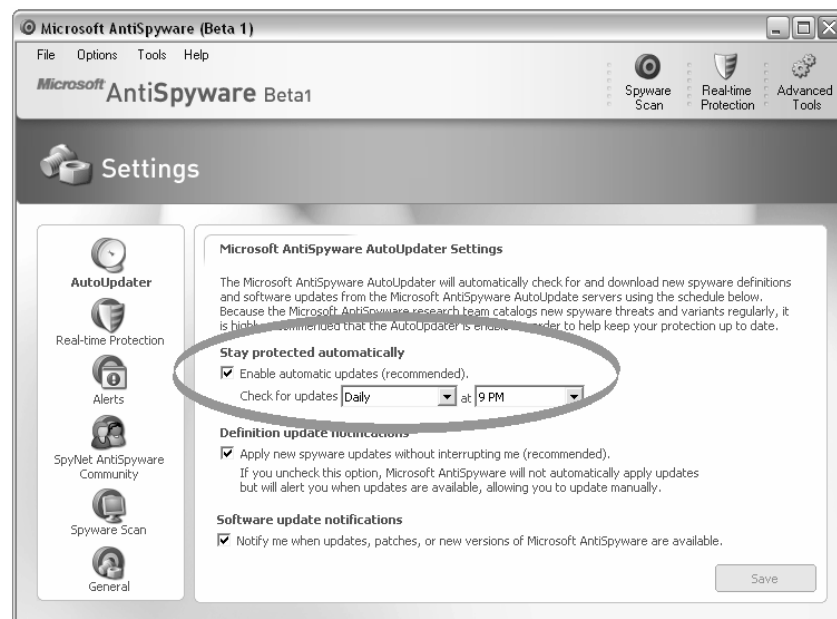
2. When the installation has been completed a confirmation message will be displayed. Click the “Close” button.

Automatic Installation

1. Select the “AntiSpyware AutoUpdater” option from the main startup screen.



2. Enable the automatic update function by selecting the check box under the “Stay Protected Automatically” heading.



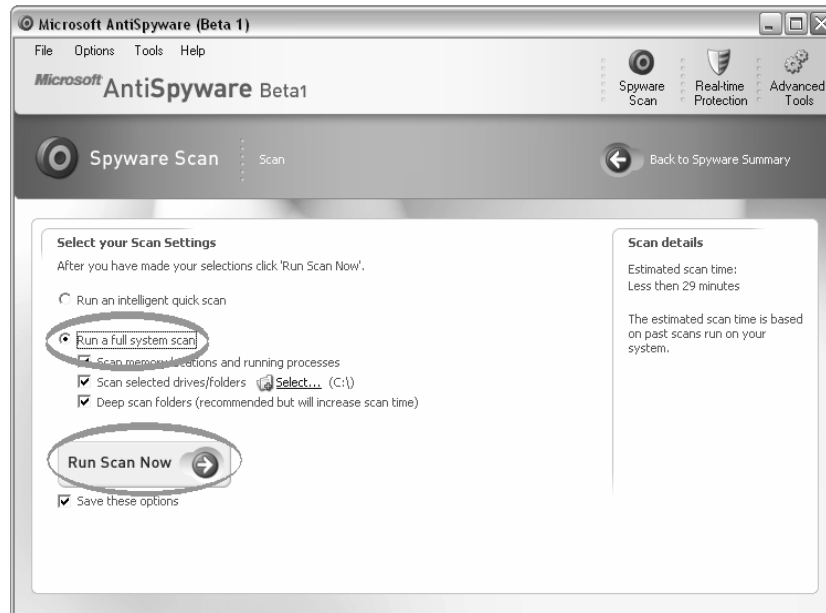
3. Click the “Save” button when finished.

Usage

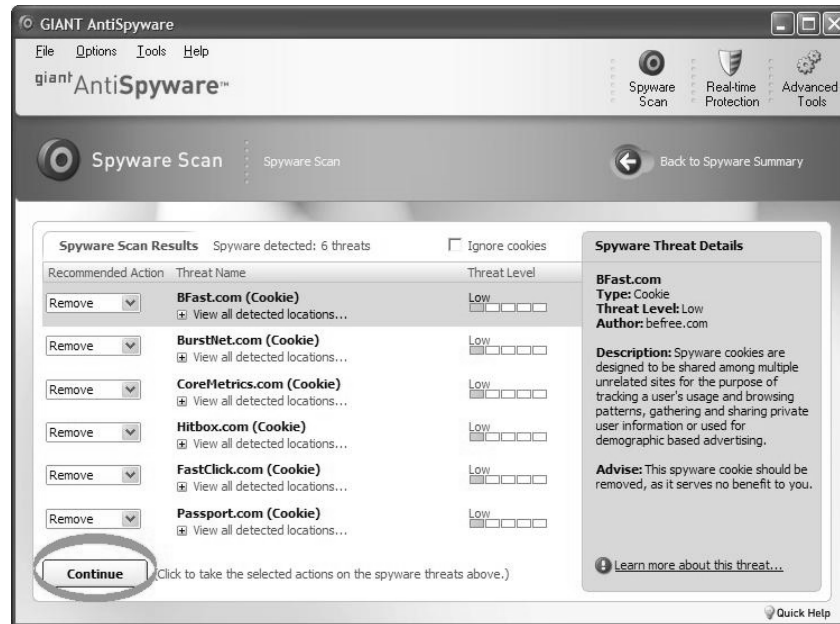
1. Click “Scan Options” from the startup screen.



2. Make sure that “Run a full system scan” is selected and click on the “Run Scan Now” button. The system scan will take several minutes to complete.



3. If any threats are found, a list of items will be displayed along with recommendations on what action to perform and a level of threat posed by the item. Review the list and be sure that the recommended actions are appropriate before selecting the “Continue” button.



4. When the threats have been removed, the process is complete. You may close Microsoft AntiSpyware.

Antivirus Software

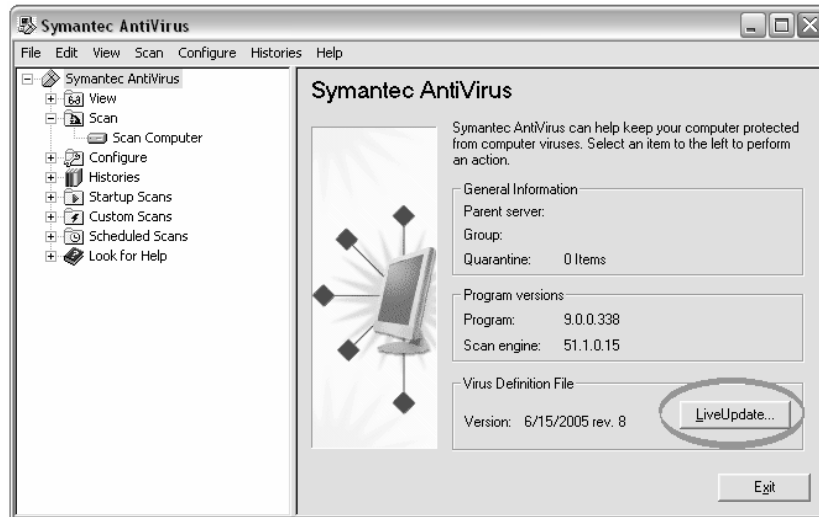
Symantec Antivirus

Begin by opening Symantec Antivirus from the programs list in the Start menu or by double-clicking on the Symantec Antivirus icon (golden shield) in the system tray.

Updates

Manual Installation

1. Click on the “LiveUpdate...” button from the startup screen.

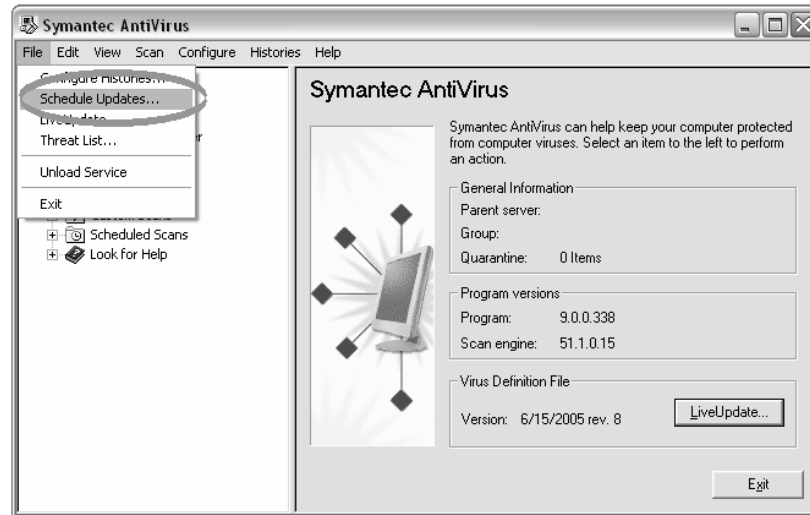


2. Click on the “Next” button in the LiveUpdate window. Live Update will contact the server to find any available updates. If updates are found, select the “Next” button; if none are found click on the “Finish” button.

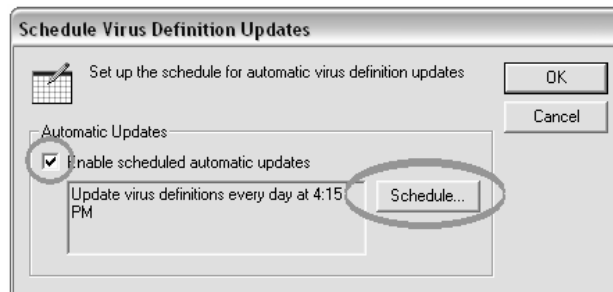


Automatic Installation

1. From the startup screen open the File menu by clicking on “File” on the menu bar.
2. Select the “Schedule Updates...” option from the File menu.



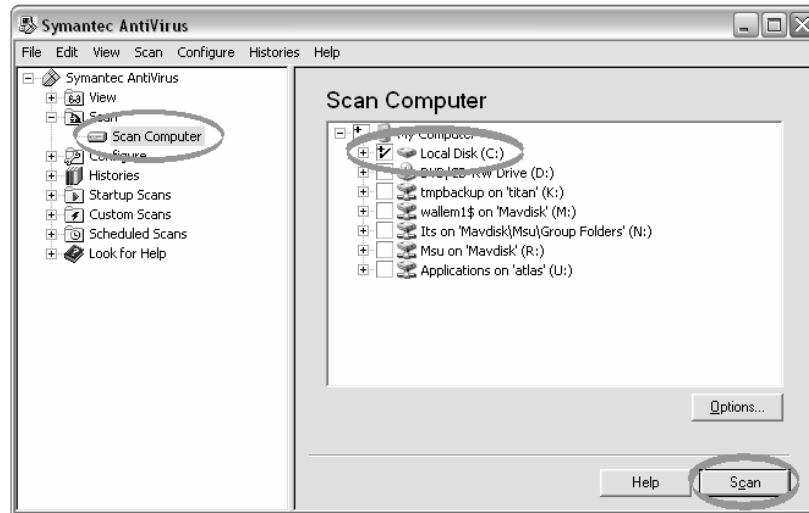
3. Make sure that “Enable scheduled automatic updates” is enabled and click on the “Schedule...” button.



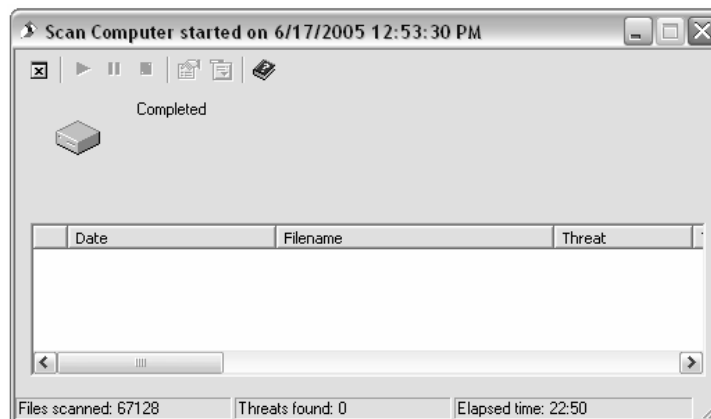
4. Select when you would like the automatic updates to run and click the “OK” button.

Usage

1. Select the “Scan Computer” option under the Symantec Antivirus heading.
2. Select “Local Disk” from the Scan Computer frame and click the “Scan” button. The scan will take several minutes to complete.



3. During the scan there may be windows that open which display information about detected virus files. Close these windows after reviewing them. When the scan is completed, a complete list of infected files will be displayed.
4. If no viruses are found close the scan window and exit Symantec Antivirus. If a virus is found, scroll to the left of the window to view what actions Symantec Antivirus performed.



5. Repeat these steps to ensure that all viruses have been removed. If infected files are still present, refer to Symantec’s website for further removal instructions.

Additional Reference Material

Where to get the software:

Ad-Aware:

<http://www.lavasoftusa.com/software/adaware/>

http://www.download.com/Ad-Aware-SE-Personal-Edition/3000-8022_4-10045910.html

Spybot Search & Destroy:

<http://www.safer-networking.org/en/index.html>

http://www.download.com/Spybot-Search-Destroy/3000-8022_4-10401314.html

Note: As you know, websites change and get updated. If these links do not work because a site has changed you can perform a search at <http://www.download.com> for both of these products and it should return the proper results. If you have any difficulty with downloading or installing this software, please contact the ITS Help Desk.

Microsoft AntiSpyware:

<http://www.microsoft.com/athome/security/spyware/software/default.aspx>

Note: You may also go to Microsoft's website and search their download page for this software.

Symantec Antivirus:

As part of the MSU community you have access to Symantec Antivirus at no cost to you. There are many ways to acquire this software. You may:

- Download it from <https://secure.mnsu.edu/downloads/>
- Check out a copy from the ITS Help Desk
- Purchase the media from the Campus Computer Store

If you have any questions about this, please contact the ITS Help Desk.

Useful Web Sites:

<http://www.symantec.com/search/>

If the Symantec Antivirus client is unable to remove an infected file, try searching this site for more information (be sure to enter the threat name given by SAV in the search field). There may be special removal instructions or a removal tool that is needed in order to clean your system.

<http://housecall.trendmicro.com>

Free online virus scan. Follow the instructions on the main page to start the scan or go directly to <http://housecall60.trendmicro.com/en/start_corp.asp>. Also available from this website is an online malware removal tool. This is available from the main page or directly at <<http://www.trendmicro.com/spyware-scan>>.

<http://vil.nai.com/vil/stinger/>

Free stand alone virus scanner available from McAfee.

<http://safety.live.com>

Microsoft's online beta of their Windows Live Safety Center. This free scan will look for safety vulnerabilities and infected files as well as remove unnecessary files from your hard drive and recommend ways to improve performance.