

Larry's newsLETTER



Techie Term: Compiler:

A program that converts programming code into a form that can be used by a computer.

Learn to read the obscure WindowsUpdate.log file

Every moment your computer is on, a nearly undocumented Microsoft file — **WindowsUpdate.log** — maintains a record of your system's patching activity.

Making sense of the information in this update log can be a challenge, but I'll show you how you can use it to learn the inside story of your PC's update history.

The **WindowsUpdate.log** file can help us determine why Windows sometimes runs "forced patches" at shutdown time — displaying none of the expected notifications that patches are available.

Microsoft's text file can appear indecipherable at first glance, but at least it's easy to locate. On any Windows computer, browse to the **C:Windows** folder to find **WindowsUpdate.log**. Note: To access this file, you may need to click **Show the files** in the right pane.

(In XP, you may see a second file named **Windows Update.log**. One file has a space in its name and the other doesn't. The one with the space is for an earlier version (V4) of the Windows Update engine. The log file without the space is the newer format and is the one you want to open.)

Open the file in Notepad or your default text editor. Make sure you start at the very top of the file. Depending on how recently and frequently a computer has been used, the log file may record activity going back several months or only a month or two. (See **FFigure 1**.)

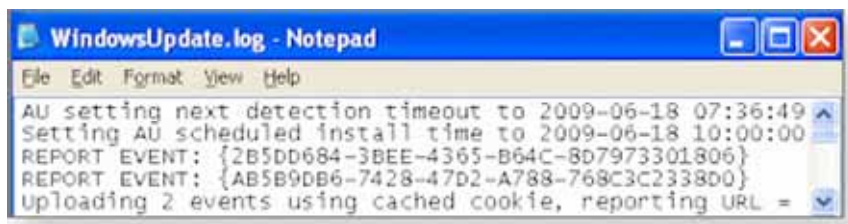


Figure 1. The **WindowsUpdate.log** file in the **C:Windows** folder records your system's update activity.

First, look for the start of the log. This records the computer's settings when it boots up and describes some of the computer's components. The following is a snippet from the top of one such file (each line of the file begins with a date and time stamp):



Larry's newsLETTER



Larry The Computer Guy

5307 Carroll Lake Rd

Commerce MI 48382

248-360-8967

- 2009-02-24 23:07:27:325 1052 46c AU ##### AU: Initializing Automatic Updates ##### 2009-02-24 23:07:27:341 1052 46c AU AU setting next detection timeout to 2009-02-25 07:07:27 2009-02-24 23:07:27:356 1052 46c AU # Approval type: Scheduled (User preference) 2009-02-24 23:07:27:356 1052 46c AU # Scheduled install day/time: Every day at 3:00 2009-02-24 23:07:27:356 1052 46c AU # Auto-install minor updates: Yes (User preference)

In line 3, the cryptic phrase "Approval type: Scheduled (User preference)" means that back on Feb. 24 — the farthest back this particular log file goes — the computer was configured to update automatically. As you'll see, this factoid can be useful to us.

Whenever you or some third-party application changes the PC's update settings, the information is recorded in the **WindowsUpdate.log** file, as shown below:

- 2009-07-03 19:01:30:531 1120 2cc AU ##### AU: Setting new AU options ##### 2009-07-03 19:01:30:547 1120 2cc AU Setting AU Approval Type to 2 2009-07-03 19:01:30:547 1120 2cc AU # Policy changed, AU refresh required = No 2009-07-03 19:01:30:547 1120 2cc AU # Approval type: Pre-download notify (User preference) 2009-07-03 19:01:30:547 1120 2cc AU AU settings changed through User Preference.

Line 2 indicates that on July 3, I changed the machine's setting for Automatic Updates (AU) to **Notify me but don't automatically download or install them**. Interestingly, the log file describes this as "Setting AU Approval Type to 2." Most Windows users, by contrast, consider this to be Option 3 in the AU dialog box. (See Figure 2.)

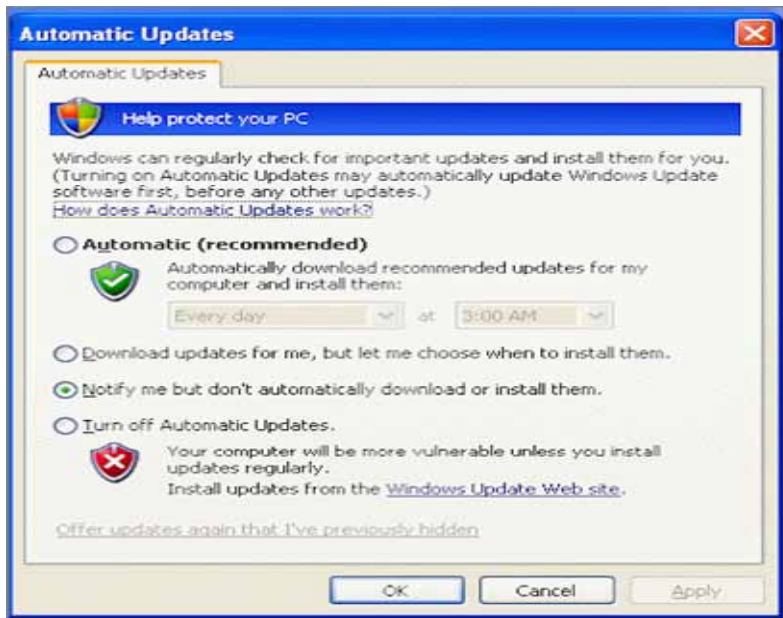


Figure 2. The WindowsUpdate.log file calls it "2," but it corresponds to Option 3 in the Automatic Updates dialog box.

Larry's newsLETTER

4 means Automatic: 3 means Download but let me choose when to install; 2 means Notify me but don't download or install; 1 means Turn off Automatic Updates.

Most important is the fact that the log file clearly records when a change was made to this setting. If patches started automatically installing, but you thought you'd made your PC require your permission, you can scan the log file to see whether your setting was changed — and possibly by whom or what.

Tracking the source of an AU settings change

When you install third-party antivirus software, the program's setup routine may change the AU setting to "fully automatic" without letting you know.

When this happens, the log file indicates that the change was made by the user, even though you may not have understood — nor even had a clue — that the change had been made.

Still, locating these change entries in the log file can help you relate a software installation to the alteration of the machine's AU setting. At the very least, this lets you eliminate other causes for the switch.

How can you find out whether patches will be installed the next time you shut down your PC? An example of such a situation is shown in the following snippet.

Near the bottom of the **WindowsUpdate.log** file for my test system — which is set to "notify me" — four patches are identified as ones that will be installed automatically at shutdown time. This doesn't mean that the four patches have been downloaded yet — merely that they're ready to be approved by the user. The entries that provide this information are as follows (notice "4 updates for install at shutdown" in line 1):

- 2009-07-09 21:38:48:625 1112 4e0 AU AU found 4 updates for install at shutdown 2009-07-09 21:38:48:656 1708 6d8 Misc ===== Logging initialized (build: 7.2.6001.788, tz: -0700) ===== 2009-07-09 21:38:48:656 1708 6d8 Misc = Process: C:\WINDOWS\Explorer.EXE 2009-07-09 21:38:48:656 1708 6d8 Misc = Module: C:\WINDOWS\system32\wuaueng.dll 2009-07-09 21:38:48:656 1708 6d8 Shutdown Install at shutdown: found updates to install

The tricky part is confirming that your log file corresponds to the update alerts you expect to see. On my test XP PC, the yellow Windows-patch icon does show up in the notification area. (In Vista, the update-alert icon is bluish-green). If I click the icon to view the available patches, I see five updates listed. Funny — these aren't the same as the four that the log file



Larry The Computer Guy

5307 Carroll Lake Rd

Commerce MI 48382

248-360-8967



Larry's newsLETTER



Larry The Computer Guy
5307 Carroll Lake Rd
Commerce MI 48382
248-360-8967

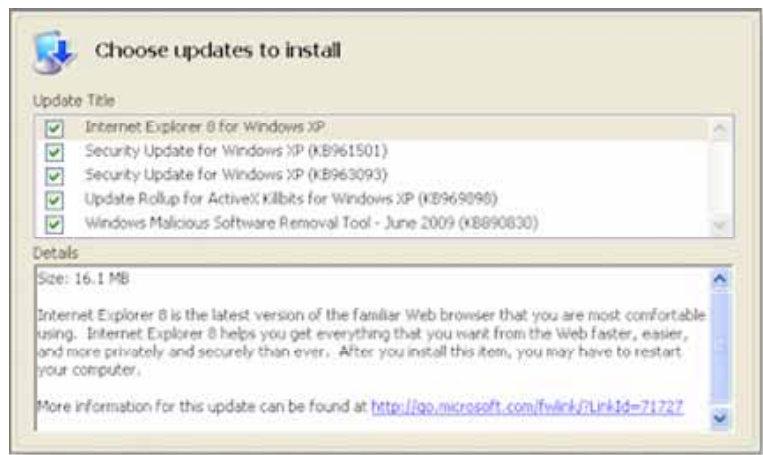


Figure 3. The WindowsUpdate.log file indicates that four updates are ready to be installed, but the selection window shows five different updates pending.

Why does the update dialog box show that Internet Explorer 8 will be installed in addition to the patches described in KB articles 961501, 963093, 969898, and 890830?

The discrepancy relates to the difference between patches being *offered* via Windows Update and those Microsoft is *pushing*.

At this writing, IE 8 is being offered as an update rather than being pushed. It may look to you as though IE 8 is going to be installed automatically. But as of today, it will install only if you select it. It will also install if you view available updates — as on my test XP PC — and fail to uncheck the IE 8 option.

Unless you read Microsoft blogs every day for fun, it's difficult to track the critical security patches — the ones being pushed — and the less-critical updates that are merely being offered.

When you choose the "notify me" option in AU, the update process is *supposed* to show an alert icon in Windows' notification area. You can click this icon to open a window in which you approve specific updates prior to installing any of them.

What if you shut down a PC without clicking the icon to select available updates? In that case, you should see a link that lets you shut down *without* installing patches this time around. (See Figure 4.)



Larry's newsLETTER

Figure 4. The XP shutdown screen indicates that important patches will be installed when you turn off the system.

In the **WindowsUpdate.log** file, the following line represents the presence of the "install-at-shutdown" warning:

- 2009-07-09 21:38:48:656 1708 6d8 Shutdown Install at shutdown: found updates to install
This line means Windows will display in its shutdown dialog box an option to control the installation of patches. To shut down without installing the pending patches — in case you want to research them further, for instance — you must choose **Click here to turn off without installing updates**. If you fail to select that option but instead click the normal Turn Off button, the updates will install automatically as the system shuts down.

A bug in the update process has been noted by many responsible observers. For some reason, Microsoft's usual "patches will be installed" indicators — the one in the notification area and the one on the shutdown screen — sometimes don't function properly. This occurs more frequently when Microsoft "throttles" its download servers, such as with the particularly large number of updates released on Patch Tuesday, June 14, 2009.

I hope my explanation of the update log will help you identify any mysterious behavior you may have experienced. Many individuals and companies must ensure that needed updates aren't installed before testing is completed for negative side-effects.

If a PC suddenly updates itself when it wasn't supposed to, **WindowsUpdate.log** can show you which settings were changed and when.

Article by Susan Bradley, WindowsSecrets.com

These documents are provided for informational purposes only. The information contained in this document represents the current view of VHC Enterprises DBA Larry The Computer Guy on the issues discussed as of the date of publication. Because VHC Enterprises must respond to changes in market conditions, it should not be interpreted to be a commitment on the part of VHC Enterprises and cannot guarantee the accuracy of any information presented after the date of publication.

INFORMATION PROVIDED IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND FREEDOM FROM INFRINGEMENT.

This newsletter and website may contain links to other websites with whom we may or may not have a business relationship. VHC Enterprises DBA Larry The Computer Guy does not review or screen these sites, and we are not responsible or liable for their privacy or data security practices, or the content of these sites. Additionally, if you register with any of these sites, any information that you provide in the process of registration, such as your email address, credit card number or other personally identifiable information, will be transferred to these sites. For these reasons, you should be careful to review any privacy and data security policies posted on any of these sites before providing information to them.

The user assumes the entire risk as to the accuracy and the use of this document. This document may be copied and distributed subject to the following conditions: 1) All text must be copied without modification and all pages must be included; 2) All copies must contain VHC Enterprises' copyright notice and any other notices provided therein; and 3) This document may not be distributed for profit. All trademarks acknowledged. Copyright VHC Enterprises, Inc. 1991-2008.

To Subscribe or unsubscribe go to www.larrycomputerguy.com and click on the mailing list link or cut and past the following link into your browser: <http://www.larrycomputerguy.com/subscribe.htm>



Larry The Computer Guy

5307 Carroll Lake Rd

Commerce MI 48382

248-360-8967