

Windows Genuine Advantage (WGA) What It Is and How to Remove It

Why WGA Is Distasteful

Just when it looks like Microsoft might be coming around, at least somewhat, on the boondoggle that is User Account Control, the company loses all rationality and releases several consecutive betas of Windows Genuine Advantage Notification, or WGA Notifications, to millions of unsuspecting Windows XP users. Moreover, it has done so via its high-priority security Automatic Updates and Windows update/Microsoft Update online-updating channels.

WGA is an anti-piracy program initiated by Microsoft in an effort to keep it from losing money on stolen product keys and counterfeit copies of Windows and Office. In typical call-it-the-opposite-of-what-it-actually-is marketing style, Microsoft has named its latest anti-piracy push to sound as if there were something good about it for customers, when in fact, the only advantage is for Microsoft. For some small percentage of legitimate Windows customers, WGA is going to be a royal pain in the behind. Make no mistake, WGA has the potential to make some people very frustrated and angry with Microsoft. And for many other people already teetering on the fence about whether Microsoft is a good company to deal with, it may tip them over the other way. If you doubt that at all, go Google "WGA."

Bloggers, newsletter authors, and computer publications have already reported a good deal about WGA. Unfortunately, the negative impact WGA may have on "man in the street" Windows users hasn't permeated into the mainstream press. It wouldn't be difficult for the New York Times, Washington Post, CNN, or Consumer Reports to find average people who've been faced with a message on their Windows XP or Office 2003 screen telling them they may have a "counterfeit copy" of their Microsoft software. Because that's what WGA does. It consists of two small bits of code. One watches your computer and tries to determine whether your copy of Windows is legit. When it decides Windows doesn't have the the proper credentials, the second component kicks in flashing warnings, and may offer you any of several pieces of advice or options, including paying up. In a way, WGA sets itself up as judge, jury, and cash register.

Microsoft has offered only vague information so far, published in a blog, about the existence of false positives — those times when WGA makes mistakes and wrongly accuses Windows customers of having an illegitimate copy of Microsoft software. At least 80% of the pirated or counterfeit software WGA finds involves the use of stolen or repeat use of one-time product keys, where Microsoft has a genuine beef. Has Microsoft (or any software development company) ever written perfect code? Of course not. So of course there are false positives. We just don't know how many.

What makes that doubly difficult to sort out — and this is the part that makes it hard for the press to report on WGA — is that not all of the apparent false positives are actually false positives. You may have paid for your copy of Windows, but it may actually be a counterfeit copy. You may have recently brought your PC in for repair, and the repair shop may have used its copy of Windows XP to reinstall Windows on your system as part of the repair process. You may have purchased a used PC sold with Windows XP or Office only to find that you weren't sold a legitimate license. In some cases, that may even happen with new PCs.

All that brings me to the aspect of Microsoft's WGA that I feel is the largest mistake. Microsoft is going directly after its own customers — not the serious bad guys — with WGA. I'm sure the software giant believes it must do this in order to get the counterfeiters, the repair shops that use the same XP CD and product key over and over again, the system builders who sell the same license repeatedly, and the smaller enterprises that, while they have purchased machines that are properly licensed, are using a single Windows image and product key (not acquired through volume licensing) for all their new PCs. But there has to be some better way than alienating probably hundreds of thousands,

Windows Genuine Advantage (WGA)

What It Is and How to Remove It

perhaps millions, of users of Microsoft software who have no idea whatsoever that they're in some way going against Microsoft's product licensing rules. The potential is huge for bad publicity, ill will, and a feeling that using Windows is an open invitation to let Microsoft decide whether you need to pay a second time for Windows or Office. Microsoft is apparently more interested in squeezing every last penny out of its existing installed base than it is in preserving customer satisfaction or developing a better mousetrap.

The actual numbers of false positives don't matter. It's about the perception. It's glaringly obvious that Microsoft cares not a whit about individual Windows users. Its only focus is larger volume-licensing customers and OEM PC makers. Since it's all about Microsoft recouping money, it's hard not to look at this as corporate greed at the expense of unsuspecting corporate customers and end users. I am personally disgusted by WGA. I'd be willing to be bet that at least half the people working at Microsoft feel the same way. They can't say it; I can.

WGA the Software

WGA software is installed into Windows XP via Microsoft's online update services. Windows Vista comes with its version of WGA already installed, apparently in no way optional. The Office version is called Office Genuine Advantage (OGA).

There are two separate parts of Windows Genuine Advantage for Windows XP: WGA Validation and WGA Notifications.

WGA Validation is the component that checks Windows to make sure it's a properly licensed copy of the software. It first appeared prior to the download of Microsoft AntiSpyware beta 1 (later renamed Windows Defender). Your system must be validated in order to receive some software (such as Internet Explorer 7, Windows Defender, and Windows Media Player 10) from Windows Update and Microsoft Update. WGA Validation has been required for access of these types of downloadable software from Microsoft since July 2005. WGA Validation is the heart of WGA. WGA Validation is not required to receive security patches from Automatic Updates. (See Microsoft's KnowledgeBase article, [Description of Windows Genuine Advantage](#), for more information about WGA Validation.)

WGA Notifications was designed to remind users who fail validation that their Windows software has been deemed by WGA Validation to be illegitimate. It directs people who experience this to resources to learn more about getting what Microsoft calls "genuine" software. WGA Notifications was rolled out this spring. WGA Notifications is delivered via Automatic Updates and it is technically optional. You can choose not to install it, but figuring out how to keep it from slipping in with high-priority security patches is not that easy (see later in this story for precise instructions on how to do that). According to Microsoft, there is no penalty for opting out of WGA Notifications. Opting out does not stop a user from receiving security updates via Automatic Updates. (See Microsoft's KnowledgeBase article, [Description of Windows Genuine Advantage Notifications](#), for more information.)

You already have WGA Validation on your Windows XP installation, unless you haven't received security patches since before July 2005. If you use the Automatic Updates feature of XP, WGA Notifications is also most likely already on your system. WGA Notifications has appeared in several beta versions, with slightly different behaviors. And Microsoft appears to be actively developing this tool. For many people, the fact that the software giant is delivering WGA Notifications, and also continues to deliver WGA Validation as needed — as high-priority security updates — is a strong note of insincerity on the part of the software giant. Microsoft may be kidding itself that WGA has some sort of security aspect, but most knowledgeable computer users aren't buying it.

At press time, when WGA detects a problem, it lets you keep running Windows, periodically popping up WGA Notifications nag screens to make sure you know that your Microsoft software may be

Windows Genuine Advantage (WGA)

What It Is and How to Remove It

counterfeit. If this happens to you, you should pursue WGA Notifications process; it may provide you with information that will help you rectify the problem. WGA Notifications may be annoying, and it does directly contact Microsoft's servers on its own, but it is WGA Validation that actually makes the determination about whether you're in license compliance. WGA Notifications is primarily a messenger, and some of its messages may be helpful.

For example, in my tests I was able to make the WGA "counterfeit" warning appear by changing the date of the system clock one month later. The Web-based WGA program was able to determine that was the problem and it suggested I reset the system date. When I did that, the WGA warnings disappeared. While most WGA detections don't resolve that easily, it can't hurt you to learn as much as you can about why WGA believes your copy Windows is illegitimate.

So what could happen? I've received several detailed reports from readers about their experiences with WGA that involves purchases of full retail copies of Windows XP from reputable dealers like Fry's, Staples, and BestBuy. The worst part of this is that there is no external review of WGA Validation's determinations. And while it's true that many people may have no idea that their copy of Windows isn't "genuine," there's no way that WGA Validation could be perfect in its determinations. One story I've heard from several readers is that they bought a retail "upgrade" installation of Windows XP Pro (from a reputable source) to upgrade a PC that came with Windows XP Home, and got into trouble after installing it. There's no way that all these copies of Windows XP Pro are counterfeit. And these people have paid the normal price for the software. It should not be up to customers to determine whether software is valid at retail. Microsoft should be able to go after counterfeiters on its own, without getting retail buyers involved.

Despite the possibility of scary messaging, WGA Notifications doesn't have much of an enforcement bite at present. But might that change in the future? Microsoft has said it won't "turn off" illegitimate copies of Windows. But could the software giant be interpreting that literally? The more likely preventive measure probably isn't turning off the computer. It's not hard to imagine that WGA might direct its predecessor, Windows Product Activation (WPA), to lock you out of your computer until such time that you can present a valid product key. When WPA kicks in, the computer boots to a login screen that doesn't let you use the computer until a valid activation code is entered. In Vista, this WPA screen links to an option that lets you buy a new copy of Windows, even extending use of Internet Explorer for that purpose, though you can't actually login to Windows prior to successful activation.

Microsoft has more than once alluded to the fact that it's reserving the right to require the installation of WGA Notifications on all computers, possibly sometime early this fall. WGA Validation and Notification are built into Windows Vista, without any user option to remove them. It's simply not known yet how Vista's version of WGA will behave.

At this writing, it is possible to both remove WGA Notifications and also to prevent it from attempting to reinstall after you have removed it.

How to Ditch WGA Notifications

There are many sites on the Internet that purport to help you remove WGA Notifications from your system. Microsoft has recently changed some things about this software, and many of those instructions could be out of date. I have yet to see a definitive work on this subject, and I don't consider this one to be either. Since WGA is still in beta, and Microsoft is still developing it, I suspect that the best set of instructions is yet to come.

A large portion of my instructions are based on Microsoft's How to disable or uninstall the pilot version of Microsoft Windows Genuine Advantage Notifications KnowledgeBase article, which showed a July 12, 2006, revision date at the time that I prepared this article. It should be noted that many of the

Windows Genuine Advantage (WGA)

What It Is and How to Remove It

simplistic methods of halting WGA Notifications, such as blocking it with your firewall or renaming the WgaLogon.dll file, are a lot less comprehensive than the instructions that Microsoft offered or that appear in this document. They are effective right now. If Microsoft renames its files, those protections would break.

The reality is, WGA Notifications isn't the guts of WGA. It's the part that "phones home." But I have to be honest with you; that aspect of WGA has never concerned me all that much. It was certainly preposterous for WGA Notifications to reach out to Microsoft's servers every day. The part of WGA that concerns me most is the virtual certainty that WGA Validation will falsely identify even a small percentage of Windows installations as being "counterfeit" when in fact they are not. OK, let's get on with removing WGA Notifications.

IMPORTANT: These instructions require editing the registry. You may want to start by taking a System Restore point so that you can revert to it in the event that something goes wrong. Also, I attempt to go beyond Microsoft's instructions for uninstalling WGA Notifications to uninstalling other WGA Notifications leave-behinds. Bottom line: I can't promise that you won't run into trouble, but I don't think you will.

Update: I've revised these instructions to work around any possible removal of WGA Validation, which is needed to download from Windows Update or Microsoft Update (though it is not part of or required for the the deliver of security patches through Automatic Updates). If you do remove it, Windows Update or Microsoft Update will reinstall WGA Validation the next time you try to use them.

To make a System Restore point, open the Start menu, choose Run, copy and paste this line into the Run field, and press Enter:

```
%SystemRoot%\system32\restore\rstrui.exe
```

If you prefer not to mess around with the System Registry yourself, there's a free utility called RemoveWGA available for download on the Internet from Firewall Leak Tester. I've tested RemoveWGA 1.2 and I recommend it as an alternative.

Removing WGA Notifications: Step by Step

1. In the Add or Remove Programs Control Panel, turn on the "Show Updates" check box at the top.
2. Open the Folder Options Control Panel. Click the View tab. Remove the check, if any, beside "Hide extensions for known file types." While you're at it, click the radio button beside "Show hidden files and folders" and uncheck the box beside "Hide protected operating system files." Click OK. (Note: If children or computer novices use your computer, you'll want to reverse these steps later.)
3. The next step is to search your entire system boot drive for any file containing the letters "wga". To do that, open the Start menu and Choose Search. You will need to configure Search so that it searches system folders, searches hidden files and folders, and searches subfolders. Initiate your search for Drive C or Drive D, or whatever drive Windows is installed on.
4. If WGA is installed on your computer, the search should return the filenames WgaLogon.dll and WgaTray.exe in your \Windows\System32 folder. You'll also find WGA's LegitCheckControl.dll in the same folder (but it won't be in your search results). You may well have several other search results, and we'll come back to those later.
5. In the search results window, rename the following two files as shown:

Windows Genuine Advantage (WGA) What It Is and How to Remove It

```
WgaLogon.dll => WgaLogon.old  
WgaTray.exe => WgaTray.old
```

- Restart your computer. Note: At this point, WGA Notifications is disabled. You could stop here if you'd rather not go all the way down this path.
- Open the Start menu, choose Run, type "cmd" without the quotation marks, and press Enter. This runs the Windows command-line console.
- In the black, command-line box, type the following line of text, then press Enter:

```
Regsvr32 %Windir%\system32\LegitCheckControl.dll /u
```

- Restart your computer.
- Use Windows Explorer (any folder window) to navigate to the \Windows\System32 folder and delete these files:

```
LegitCheckControl.dll  
WgaLogon.old  
WgaTray.old
```

- Open the Start menu, choose Run, type "regedit" without the quotation marks, and press Enter. This opens the Registry Editor.
- Locate and delete the last subkeys (folders) in these locations in the Registry. (Note: HKLM stands for HKEY_Local_Machine.)

```
HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Notify\WgaLogon  
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WgaNotify
```

Note: Just to be clear, for that first line, you would navigate through the Registry beginning with HKEY_Local_Machine area, tunneling in by opening each folder named in the Registry path until you see the WgaLogon folder on the left side of the Registry Editor. Then just delete that folder. Repeat for the other Registry subkey, WgaNotify.

- That ends Microsoft's initial instructions. On my computers, I reboot my computer and remove the following subkeys as well. You should not attempt to remove every instance of WGA in the Registry.

```
HKLM\SOFTWARE\Microsoft\Updates\WgaNotify  
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Management\ARPCache\WgaNotify
```

- The next step is to delete other WGA Notifications files returned in your search. It's not absolutely essential for you to remove every last trace of WGA Notifications, especially when that attempt could very likely get you into trouble. For example, wgaapi.dll isn't part of Microsoft WGA, it's part of a wireless networking driver. You can safely delete any file you find with "wganotify" in its name.

On several of my computers I didn't find WGA installed, but I did find an installer for it that seemed poised to run the installation. Presumably that's because those computers were using the Automatic

Windows Genuine Advantage (WGA)

What It Is and How to Remove It

Updates setting that automatically downloads but does not install updates without your permission. They're usually located in a folder with a name consisting of gobbledy-gook (hash of alphanumeric characters) found the \Windows\softwaredistribution\download folder. It's possible to delete these folders, but remember that WGA Validation and WGA Notifications are different things, and you need WGA Validation to get security patches. Folders that contain WgaTray.exe and/or WgaLogon.dll are for WGA Notifications. When in doubt, leave them as is.

You may find that the operating system blocks you from deleting these folders. If so, you can either reset the file object permissions (assumes you have Windows XP Pro with the NTFS file system and you're running with Simple File Sharing turned off) or you can boot into Safe Mode and try deleting them there. If you're not sure how to do these things, it is truly not worth bothering with. Leave well enough alone.

Preventing Recurrences

You're not quite done yet. If you don't follow this next set of steps, you could find WGA installed on your system a couple of days later.

1. Change the Automatic Updates Control Panel setting to "Notify me but don't automatically download or install them." From now on, you will need to closely monitor every update that Microsoft wants to install on your computer.
2. Wait for the yellow shield icon to appear in your system tray that signifies that updates are available. This can take as much as two days, but it's usually only a couple of hours.
3. Click the yellow icon and, if prompted, choose the "Custom Install" option, which will bring up the "Choose updates to download" dialog.
4. Remove the check mark beside any entry that contains the words "Windows Genuine Advantage" and click Close. (If there are other security updates waiting to install too, leave their check marks in place and they will continue to be available later.)
5. Yet another box will open labeled Hide Update. Remove the check mark beside "Don't notify me about these updates again."

Some WGA Resources

These additional sources of information are required reading about WGA:

- Truth and Distortion About Microsoft's WGA - Computerworld Blog
- Ed Bott's Microsoft Report - ZDNet
- Windows Genuine Advantage FAQ
- Windows Genuine Advantage Talkback Forums - Microsoft