« TweakUAC: Don't Get Mad, Get Even! Disable annoying Vista pop-ups with this free tool.
TweakUAC updated for Windows Vista RTM »

Am I at risk if I disable UAC?

To understand the ramifications of disabling UAC (User Account Control of Windows Vista), let's consider the threats it is supposed to protect us from. Here is what Microsoft has to say about it on their User Account Control Overview page:

"The main goal of User Account Control is to reduce the exposure and attack surface of the operating system by requiring that all users run in standard user mode. This limitation minimizes the ability for users to make changes that could destabilize their computers or inadvertently expose the network to viruses through undetected malware that has infected their computer."

In other words, if a virus infects your computer, UAC is designed to reduce the impact of it on the operating system. While that's a good thing, note that UAC does not prevent your computer from being infected with the viruses in the first place, it can only reduce the possible damage caused by the infection. It means that we still have to have anti-virus and anti-spyware software running on our computers (and keep them up to date!) And let's not forget about the firewall, it's just as important as antivirus for keeping your computer out of reach of the bad guys.

Let's re-read the Microsoft's statement once again. Note that UAC is not designed to protect your personal files from the viruses, it only protects the operating system. That is, if a virus gets into your computer with UAC enabled, it will still have the full ability to damage your documents, or to collect all email addresses from your address book and send email messages to everyone pretending to be you, and so on. Even if your files are encrypted, a virus will have full access to them just like you do, even if it runs with the limited privileges of a standard user. Think of it this way: everything you can do with your computer as a standard user, a virus can do, too, and UAC cannot stop that on its own.

But if UAC protects the operating system from the virus, that must be a good thing, right? Of course it is, but while preventing viruses from attaching to system files was important in the old pre-Internet days, viruses no longer spread themselves that way: when was the last time you copied a system dll on a floppy and gave it to a friend who asked to help him repair his installation of Windows?

As for limiting the ability of a virus to start automatically every time Windows Vista starts (another activity UAC is designed to protect from), such ability gives the virus almost no advantage, because restarting a Vista computer is a very rare event (after it is initially configured and set up). Even if you press the Turn off button on the Start Menu, and then turn the computer back on, the regular operating system restart does NOT occur: Vista simply hibernates the computer and then wakes it up, rather than going through the complete restart routine. It means that it may be days or weeks or even months before Vista gets actually restarted, and all this time a virus in your computer can be active and operational, even without the ability to install itself to auto-run on Windows restart. So, even if UAC keeps the virus from doing that, it does not prevent the virus from running for the extended periods of time.

And let's keep things in perspective: what is more embarrassing, having a virus send a bunch of emails from your name to every address in your address book, or attach itself to a system dll? Or, what is more damaging, a virus erasing your documents or installing itself to run automatically at Windows start-up? Guess what, I could not care less about the operating system, I can reinstall it from scratch any time I want. Sure, it would take a couple of days and cause a lot of frustration, to reinstall Windows and all applications I use, to configure

Let me reiterate once again: to be protected from viruses, we still need the anti-virus software and a firewall, because that's where the real protection is, no matter whether UAC is enabled or not.

One area where UAC can actually serve a useful purpose is, as stated on the Microsoft's web page I mentioned above, to minimize the ability of users to destabilize their systems by making changes to the global settings of the computers. This is a good thing for the users who get new computers with the administrative accounts set up for them by default, but who do not have enough computer knowledge and experience to make significant changes to the global computer settings. In such a case, UAC can keep the user from messing up his or her system, for the user's own good. However, even in this case the effectiveness of UAC is limited: after the user learns to click on the Allow button to continue with the task, after a while s/he will be clicking on it automatically, without paying much attention to the text of the message. And that opens a possibility for the malware to trick the user into allowing it to run with the administrative privileges: after all, can you expect an average user to read and analyze the text on the elevation prompt every time it pops up on the screen?

Another area where UAC could be of use is when Vista is installed on a public computer, where anyone can walk in to the computer and mess it up. However, that's what the limited user accounts are for: you would be insane to allow everyone to access a public computer via an administrative account, even with UAC enabled on it! That means that even for the public computers UAC is essentially a useless addition.

So, would it be wise for you to disable UAC? Ultimately, it's for you to decide, whether the thin layer of extra protection that UAC provides is worth the extra annoyance it adds to your work. Hopefully, this article will help you make the right choice.

Andrei Belogortseff
WinAbility Software Corp.

Share it:

- 
- 
- 
- 

This entry was posted on Thursday, September 28th, 2006 at 2:35 pm and is filed under TweakUAC. You can follow any responses to this entry through the RSS 2.0 feed. You can leave a response, or trackback from your own site.

5 Responses to "Am I at risk if I disable UAC?"

1. *pnx* Says:
   December 12th, 2006 at 9:11 pm

   I seriously believe you are sending out a dangerous message with the above post. First you are correct, UAC does not protect USER files, and does focus on system files and dll's. From your comments of "Guess what, I could not care less about the operating system" seem to be very nieve. For starters, if mallicious code decides to attach itself to a system dll and hook all website requests to popular banking websites, intercept emails, log passwords etc… I believe this to be much more of an issue then simply spamming your address book !!!!

"after the user learns to click on the Allow button to continue with the task, after a while s/he will be clicking on it automatically, without paying much attention to the text of the message" -> So what is the answer then ?? A new windows vista that reads minds ?? Or maybe written concent after studying the program functionality? At the end of the day microsoft have implimented this feature for security, if the user decides to disregard the messages then who's fault is that !?!

2. *Andrei Belogortseff* Says:
December 13th, 2006 at 7:27 pm

Thank you for your feedback. Please see my reply here:

http://www.tweak-uac.com/dont-kill-the-messenger/

3. *pnx* Says:
December 19th, 2006 at 5:34 pm

First let me thank you for replying to my above comment, and the points that you relay in your reply have been taken on board…..

…..but I still reinforce my original statements. UAC is not the be-all and end-all in computer security (I don't pretend this to be true), but compared to what we had previously (where all exe's were granted full access to opening system files, (until recently) shifting through raw system memory, infecting other processes memory spaces etc..) I believe it to be a big improvement.

Surely it is a lot easier to teach someone, "well if this UAC box pops up, it means that the program may do something harmful", rather than saying "well if you double click on this exe, then it may do something harmful, but there again it may not". UAC is a feature added as an optional for programmers. If programmers require access to privileged resources on an OS then they have to include a suitably tuned 'manifest' resource in order to access those resources, and thus the UAC box pops up requesting access (kinda like an auto sudo command in linux). Again, if the programmer does not require resources on the OS, then the manifest can be tuned to reflect this also (or left out completely) and no UAC box will be shown.

This feature was added to help users, and in my opinion it has. The average user just has to be told what the UAC box is for. As for your comments of 'the user should not be responsible and the OS should check everything', well can you imagine what that would be like, heuristic scanning on every exe the user opens. Every two seconds the system would cry wolf (and if you think UAC is bad). This used to be quite effective once upon a time when it was only virus writers using such odd techniques in their creations, but now with file packers and anti piracy tools about many legitimate programs use similar techniques (just try running your AV heuristics and you will see).

Well thats all for today and I apologise if any of my above comments seem a little patronizing, but I kinda thought its best assuming no skill at all so that way everyone understands (hey, kinda like UAC).

but….. Progress has to start somewhere.

4. *Anonymous* Says:
September 6th, 2007 at 11:08 am

The point of ther UAC prompts is that they are hosted on a secure desktop so that it is impossible for malware to click the 'yes' buttons for you.

5. *David Guinness* Says:
   November 22nd, 2007 at 4:11 pm

   Andrei,

   I would like to thank you for your work on this program. I've found its features very helpful. I consider myself a well-informed Vista user, and because I am careful with my internet security and the applications I run, I have found very little benefit to UAC, and have certainly experienced enough frustration with it. However, I didn't want to turn it off. Therefore I appreciate your approach to suppress it, rather than to disable it altogether.

   Best of luck to you, and a very happy Thanksgiving,
   David Guinness

Leave a Reply

Name (required)

Mail (will not be published) (required)

Website

To prove that you are a human being and not an automated spambot, please answer the following question:

What is the result of 3 plus 3:

Submit Comment

- Search
-

- # Pages

  - Home
  - What is UAC?
  - What is TweakUAC?
  - Download
  - License (EULA)
  - About

- Vista Elevator 1.0
- Vista Elevator 2.0

Our software

- Folder Guard
- AB Commander
- Active Exit
- MySecretFolder
- Desktoplet
- ... and more!
