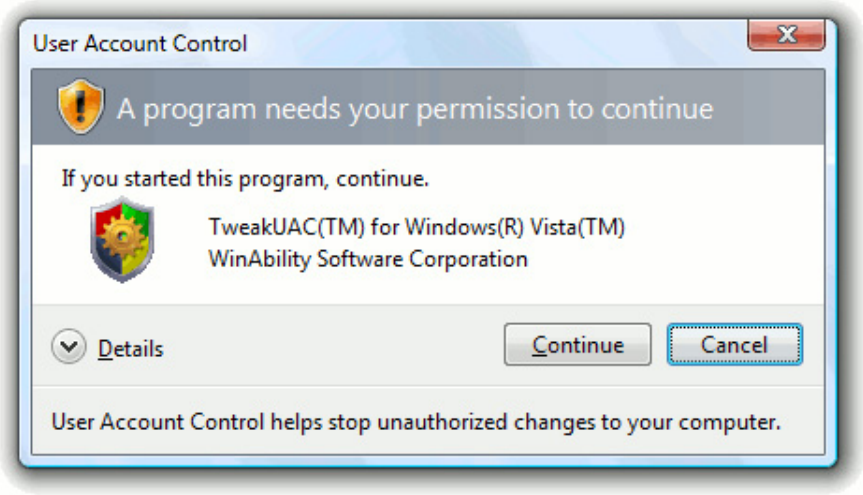
4 reasons why Windows UAC is useless

If you have been using Windows Vista or Windows 7, you will probably feel a lot of pain when you have to get the system approval every time you install an application. This feature is called User Account Control (UAC), ...

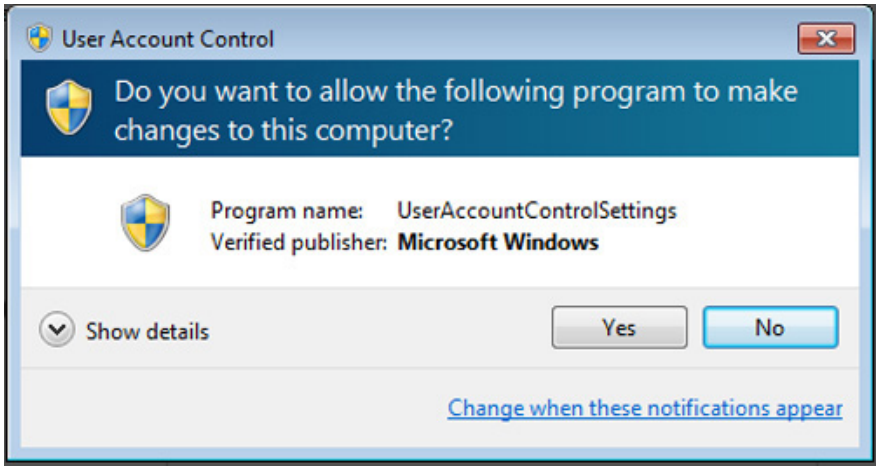
TipsMake.com - If you are already using Windows Vista or Windows 7, you will definitely feel a lot of pain when you have to get the system approval every time you install an application. This feature is called User Account Control (UAC), which provides a dialog box that pops up whenever something is opened. Microsoft has created UAC for the purpose of making computers more secure for end users and similar technicians.

>>>**Discover UAC of Windows 7**



If you are a ' *victim* ' of this ' *security measure* ', you will know why this is Microsoft's failure. That indicates that UAC can even interfere with system security at home and in the office. The following 4 reasons why we do not need to turn on UAC feature (refer to the article: **Ignore the UAC warning by creating a shortcut with Administrator rights**).

1. Everyone clicks 'Yes'



Even if there are rows of text pages bolded on the screen, the average home user will click ' **Yes** ' if any dialog box appears. This is the case known as a reflex, and develops in repetitive behaviors. Let's face it! The majority of applications on your computer are safe. If up to 98% of applications opened in a computer is safe, only 2% can be punished by end users clicking ' **Yes** ' on the dialog box that appears. Imagine you can spend 8 hours a day reading 200 dialogs, if you don't get paid for this?

2. The person is complacent / frustrated

UAC does not work as expected, but it is annoying, for this reason, to make it unreliable. Some advanced users will disable UAC manually, then teach their friends how to do it. Even for new users, they will forget that UAC is a security feature and try to disable it to avoid nuisance. This leads to an increased risk of security vulnerabilities and Microsoft will not compensate if users do not install an antivirus application.

3. The effect is not correct but expected

If you've ever been infected with a malicious infection while UAC is still enabled, then you'll know the truth. UAC does not protect you against malware, since there are different ways to call the Windows function library (WINAPI) without actually going through this feature's screening process. The simple method that malware uses to bypass security features is to create similar actions to an ' *innocent* ' application, then write it all to your **AppData** folder without touching it. UAC.

4. Not everyone knows about Malware

It's not something that looks like a vampire or the Jolly Roger logo (skull-shaped flag icon) for users to recognize. Most people will look at things like ' *Internet Optimizer* ' and mistakenly think of it as a harmless application name and then accidentally click ' **Confirm** ' in the UAC dialog if they read the text on it. Malware will be infecting computers and it is an agreement made. Windows has no way to tell you: ' *Hey, look at this! We think it's malware!* '

Conclude

While the purpose of UAC is good, it also often gives people a false sense of security, or worst is offensive to all of us. We do not recommend you to completely turn off UAC, but it is never safe when you click the ' **Continue** ' button without thinking about the consequences!

You finished reading the article "**4 reasons why Windows UAC is useless**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
