

Windows7安全之根本：UAC详解Microsoft认证考试 PDF转换可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/644/2021\\_2022\\_Windows7\\_E5\\_AE\\_c100\\_644641.htm](https://www.100test.com/kao_ti2020/644/2021_2022_Windows7_E5_AE_c100_644641.htm)

UAC是什么？在本文之前，建议先阅读一篇老文章《软媒原创：如何从根上保证电脑安全、不中毒》。UAC (User Account Control)，中文翻译为用户帐户控制，是微软在Windows Vista和Windows7中引用的新技术，主要功能是进行一些会影响系统安全的操作时，会自动触发UAC，用户确认后才能执行。因为大部分的恶意软件、木马病毒、广告插件在进入计算机时都会有如：将文件复制到Windows或Program Files等目录、安装驱动、安装ActiveX等操作，而这些操作都会触发UAC，用户都可以在UAC提示时来禁止这些程序的运行。能够触发UAC的操作包括：\* 修改Windows Update配置；\* 增加或删除用户帐户；\* 改变用户的帐户类型；\* 改变UAC设置；\* 安装ActiveX；\* 安装或卸载程序；\* 安装设备驱动程序；\* 修改和设置家长控制；\* 增加或修改注册表；\* 将文件移动或复制到Program Files或是Windows目录；\* 访问其他用户目录

UAC很烦 是的，微软自从Windows Vista开始加入了UAC，这也成了人们对VISTA不满的诟病之一，因为Vista不像Win7一样可以对UAC进行级别设置（其实Windows7的UAC也很烦），当时的电脑的普遍配置也很低，所以人们对这个动不动就弹出来，同时还会锁定屏幕的家伙很厌恶。UAC在Windows 7中的完善就是因为UAC太烦了，所以微软在Windows 7中，加入了UAC的等级设置功能，分别对应4个级别：最高级别：在高级级别下，“始终通知”（即完全开启），在该级别下，用户安装应用

程序、对软件进行升级、应用程序在任何情况下对操作系统进行更改、更改 Windows 设置等情况，都会弹出提示窗口(并启用安全桌面)，请求用户确认。由此可见该级别是最安全的级别，但同时也是最“麻烦”的级别，适用于多人共用一台电脑的情况下，限制其他标准用户，禁止其随意更改系统设置。

**默认级别：**在默认级别下，只有在应用程序试图改变计算机设置时才会提示用户，而用户主动对 Windows 进行更改设置则不会提示。同时，在该模式下将启用安全桌面，以防绕过 UAC 更改系统设置。可以看出，默认级别可以既不干扰用户的正常操作，又可以有效防范恶意程序在用户不知情的情况下修改系统设置。一般的用户都可以采用该级别设置。

**比默认级别稍低的级别：**与默认级别稍有不同的是该级别将不启用安全桌面，也就是说有可能产生绕过 UAC 更改系统设置的情况。不过一般情况下，如果用户使用户启动某些程序而需要对系统进行修改，可以直接运行，不会产生安全问题。但如果用户没有运行任何程序却弹出提示窗口，则有可能是恶意程序在试图修改系统设置，此时应果断选择阻止。该级别适用于有一定系统经验的用户。

**最低的级别：**最低的级别则是关闭 UAC 功能(必须重新启动后才能生效)。在该级别下，如果是管理员登录，则所有操作都将直接运行而不会有任何通知，包括病毒或木马对系统进行的修改。在此级别下，病毒或木马可以任意连接访问网络中的其他电脑、甚至与互联网上的电脑进行通信或数据传输。可见如果完全关闭 UAC 并以管理员身份登录，将严重降低系统安全性。此外，如果是标准用户登录，那么安装、升级软件或对系统进行修改和设置，将直接被拒绝而不弹出任何提示，用户只有获得管

理员权限才能进行。可见完全关闭UAC并以标准用户登录，各种操作和设置也非常不方便，因此建议不要选择该级别。但是UAC很有用 UAC虽然经常安装软件的人很烦，但UAC的作用却不容小觑。不得不承认微软对于操作系统的理念是很超前的，所以经常会搞出一些虽然很棒却很尴尬的东西，就好像当年的VISTA，在人们开始接受Windows 7的今天，再回头去看Vista，才越来越意识到VISTA其实是一个很不错的操作系统，只不过是生不逢时。更完善的安全机制在木马病毒变种越来越多，越来越快的今天，杀毒软件对系统安全的作用越来越有限，我们越来越需要一些全方位的系统防护软件，如目前很多杀毒软件已经加入的防火墙、防间谍、保护敏感数据、文件粉碎机等等。微软在Windows 7更好的完善了安全机制，提供了Windows Update、内置防火墙、Windows Defender、UAC、MSE、Bitlocker等安全功能组件。其中：

- \* Windows Update可以更新系统补丁，及时修复系统漏洞；
- \* 防火墙可以阻止一些网络攻击和信息泄露；
- \* Windows Defender可以清除一些已被定义的恶意软件；
- \* UAC可以协助用户阻止一些未定义的恶意软件、木马的运行；
- \* MSE是微软官方提供的免费杀毒软件，可以清除病毒；
- \* Bitlocker是微软给企业用户及Windows Ultimate（旗舰版）用户提供的专业级加密系统，可以对敏感数据进行加密，防止资料和数据外泄。

这些安全组件相结合，才能打造一个更好的系统安全环境，其实合理利用Windows7自带的如系统还原和备份、策略组、PowerShell等功能，都可以对系统安全起到很好的作用。

优化的误区 从Windows XP起，系统优化就是一个很热门的话题，网上可以搜到很多关于优化的文章。可是系统优化，要

因人而异，盲目的优化只能适得其反。很多优化的文章上来就教人怎么关闭Windows自带的各种功能，如关闭UAC，却很少告诉别人这个功能的用途，美其名曰可以加入系统速度，却不知道这样做会造成很多隐患，也失去了体验Windows新功能的机会，结果往往是得不偿失。信息安全的木桶原理一个木桶能装多少水，不是由那些长板决定的，而是由那块最短的板决定的，这就是著名的“木桶原理”。同样适用于信息安全，其中任何一个环节的失败，就是全盘的失败。假如当年陈冠希把他的“数据”通过文件粉碎删除，或使用Bitlocker加密一下，我们就不会有“大饱眼福”的机会了。安全，最重要的还是你自己这是引用了我以前的一篇文章的标题，这个世界没有无缘无故的爱，也没有无缘无故的恨，我用这句话来解释为什么装了同样的杀毒软件，很多人经常中病毒，而有些人却很少中病毒的原因。是因为很少中病毒的人有很好的安全意识和操作习惯，还有很重要的一点是能够利用各种除杀毒软件以外的工具来保障系统安全。多学习、多了解、多实践，才是关键，不妨打开你的UAC，去好好体验一下这项功能吧。相关推荐：[#0000ff>禁用Mcafee2010自动生成桌面图标](#) [#0000ff>Windows7下关闭IPV6隧道](#) [#0000ff>两步轻松还原Windows7的默认字体](#) [100Test 下载频道开通](#)，各类考试题目直接下载。详细请访问 [www.100test.com](http://www.100test.com)