

Windows Vista

使用教程



第三章 UAC(用户帐户控制)

Ver 0.2

声明:

- 1、 本电子文档可能不是Windows Vista使用教程的最新版, 请至[Vista天地](#)查看更新
- 2、 您可以在保证本文档完整性的前提下传播、复制、使用本文档(限非商业性使用)

目录：

[目录列表](#)

[第一章：安装、升级与卸载](#)

[1.1 安装前的准备](#)

1.1.1 Windows Vista 的硬件要求

谨慎看待微软的 Windows Vista 徽标认证

使用 Windows Vista 升级顾问检查硬件

使用 Windows 体验索引衡量硬件性能

1.1.2 Windows Vista 推荐配置

1.1.3 选择合适的 Windows Vista 版本

1.1.4 选择合适的安装方式

[1.2 安装Windows Vista](#)

1.2.1 硬盘分区、驱动及其他

硬盘分区

驱动程序

双重启动或多重启动

1.2.2 图解 Windows Vista 安装

1.3 个人设置与用户数据的迁移

[1.4 卸载Windows Vista](#)

Windows Vista 是 PC 唯一操作系统时的卸载

Windows Vista 与其他操作系统共存时的卸载

卸载 Windows Vista 的简单办法

多重启动环境下的卸载

[第二章：基本操作](#)

2.1 桌布与外观

新的桌面，新的名称

边栏与小工具

消失的“文件”菜单

2.2 开始菜单

开始菜单内置搜索

关机按钮预设为睡眠而不是传统意义上的关机

2.3 无处不在的搜索

2.4 全新的资源管理器

2.5 网络与共享

2.6 系统设置与调整

程序相关

桌面设置

[第三章：UAC\(用户帐户控制\)](#)

3.1 UAC 的目标与策略

3.2 UAC 机制简解

3.3 UAC 无处不在

3.4 安装程序、下载文件与 UAC

3.5 更改 UAC 的提示方式

[第四章：网络与共享](#)

4.1 [网络基础](#)

4.2 [网络和共享中心](#)

4.3 [共享](#)

4.4 [网络相关的其他设置与操作](#)

与之前的Windows版本如Windows XP相比，Windows Vista所带来的改进是全方位的，但要说到在操作方面带来的最大变化，恐怕非UAC(User Account Control：用户帐户控制)莫属。

因此，虽然之前[Vista天地](#)对UAC已经作出相当多的介绍，如从机制与原理方面的[Vista中的UAC：用户帐户控制](#)、[UAC为Windows Vista带来了什么?](#)以及具体的操作方法如[关闭Windows Vista中的UAC](#)等，但对[Windows Vista使用教程](#)而言，单独地以一章的篇幅再来详细介绍一下UAC 总是不可或缺的。

本文对 UAC 的介绍侧重于从操作、使用方面，更详细的信息请参考 Vista 天地的其他相关内容。

3.1 UAC 的机制、目标与策略

Windows 系统因其庞大的市场占有率成为各类恶意软件、病毒觊觎的首要目标，各式各样针对 Windows 系统的攻击手段与技术层出不穷，这是微软的成功但也是微软最大的悲哀：以一家企业之力来对抗全世界狂热的“攻击爱好者”，只能是防不胜防疲于奔命，这也直接造成了在许多用户印象中 Windows 是一款相当脆弱的操作系统的印象。

当然，这么说并不是为微软开脱。从技术角度看，Windows 为了保证易用性与用户友好度，在安全性方面所付出的代价过大，存在着致命的缺陷，其中最引人诟病的当属用户级别与执行权限的问题。比如说，相信许多朋友都曾或多或少地受过“流氓软件”的骚扰，许多人甚至谈“网”色变，形成这么恶劣的上网环境，微软难逃其咎——当然，流氓软件之所以在国内泛滥，也与某些“民族企业”缺乏最基本的道德准则有关——以最普遍的插件类流氓软件来说，虽然其并没有太高的技术含量，但却往往能轻易地突破 Windows 系统的防御，最大的问题便在于 Windows 系统如 Windows XP 标准帐户存在的诸多问题而使得用户为操作的使得而使用超级用户登录，从而使流氓软件轻易地获得权限。

UAC(User Account Control：用户帐户控制)是微软为提高系统安全性而在 Windows Vista 中引入的新技术，其设计目标便是防止间谍软件或病毒程

序在用户电脑系统中获得权限并在用户未察觉的情况下执行。在 UAC 的作用下，当 Windows Vista 检测到某个未知的潜在威胁时，便会弹出一个“Windows 需要你的许可才能继续！”的对话框，提醒用户注意或并根据具体情况允许/阻止其执行。

简单地说，UAC 机制的核心在于：Windows Vista 要求所有用户在标准帐号模式下运行程序和任务，这样，当相应的程序或任务执行可能会影响计算机运行的操作或执行更改影响其他用户的设置的操作，即需要/试图获得高出标准帐号权限时，系统即会弹出相应的警告信息并等待用户确认及赋予权限，从而阻止未认证的程序安装，或者阻止标准用户进行不当的系统设置改变。

很显然，通过引入 UAC，Windows Vista 在安全性方面有了很大的改进，但同样地，UAC 机制本身给用户操作顺畅度带来的负面影响也是不容回避的：即使具有很好耐心的用户，也可能被日常操作中频繁弹出的 UAC 窗口打断颇有微辞，以至于很多用户考虑[在 Windows Vista 禁用 UAC](#)或[绕过 UAC 开启超级管理员](#)。——当然，从系统安全性的角度考虑，这绝不是一个明智的选择。

对微软来说，在系统安全与系统操作的流畅间如何找到最佳的平衡点，也许仍是一个长期的工作，UAC 也许还需要谨慎、细致的调整。

3.2 UAC 机制简解

在 Windows Vista 中，默认有两个级别的用户组，即标准用户组和管理员组，其中，标准用户是计算机 Users 组的成员；管理员是计算机 Administrators 组的成员。

而微软在 Windows 所做的改进在于，与以前版本的 Windows 不同，默认情况下标准用户和管理员都会在标准用户安全上下文中访问资源和运行应用程序。这样，当用户登录到计算机后，系统为该用户创建一个访问令牌。该访问令牌包含有关授予给该用户的访问权限级别的信息，其中包括特定的安全标识符 (SID) 和 Windows 权限。

如果登录用户属于管理员组，则 Windows Vista 为该用户创建两个单独的访问令牌：标准用户访问令牌和管理员访问令牌。标准用户访问令牌包含的用户特定信息与管理员访问令牌包含的信息相同，但是已经删除管理 Windows 权限和 SID，用于启动不执行管理任务的应用程序。而当运行执行管理任务的应用程序时，Windows Vista 提示用户将他们的安全上下文从标准用户更改或“提升”为管理员，这一过程被称为“管理审核模式”。只有在此该模式下，应用程序需要特定的权限才能以管理员应用程序(具有与管理员相同访问权限的应用程序)运行。

默认情况下，当管理员应用程序启动时，会出现“用户帐户控制”消息。如果用户是管理员，该消息会提供选择允许或禁止应用程序启动的选项。如果用户是标准用户，该用户可以输入一个本地 Administrators 组成员的帐户的用户名和密码。





3.3 UAC 无处不在

在 Windows Vista 中, UAC 遍及系统的各个角落。事实上, 只要在 Windows Vista 进行操作, 便可时不时地遇到以小盾牌标注的 UAC 操作提示, 比如说在控制面板中:



再或在文件夹属性页中的“高级共享”设置：



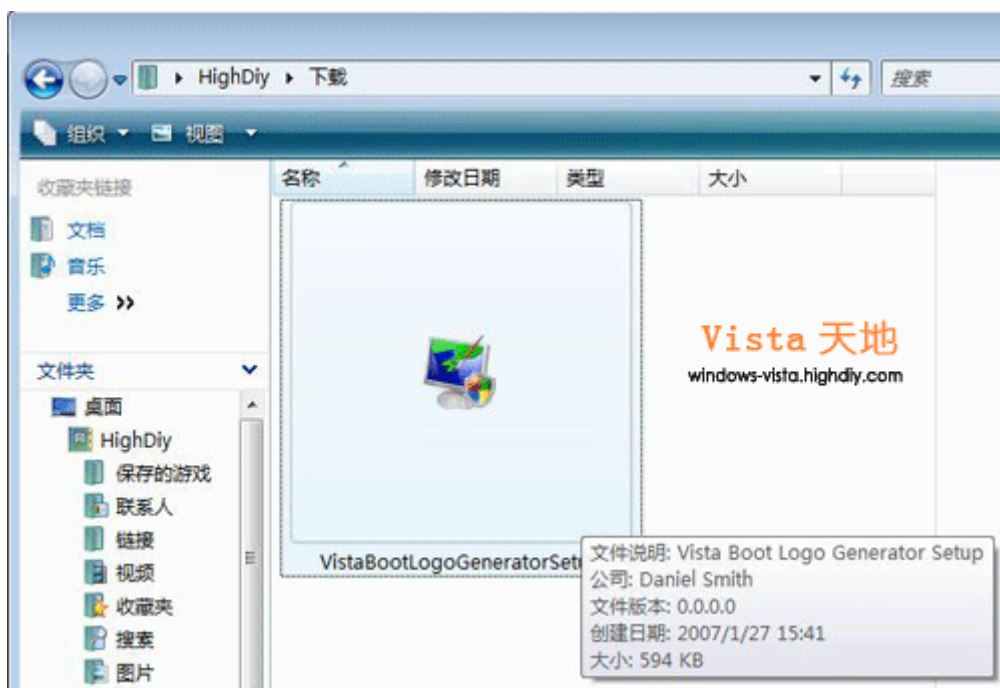
当点击这些以小盾牌标注的操作项时，系统即会触发 **UAC**，弹出相应的权限提升及确认窗口，根据登录用户身份的不同，会有上节介绍的两种提示窗口。此时用户需输入管理员密码(标准用户)或确认是否允许执行(管理员)。

需要指出的是，在弹出的 **UAC** 窗口中，按键焦点默认为“取消”，即如果允许该程序/服务执行，用户需手动选定“确定”按钮，这也可在一定程度上避免用户不小心误操作存在的风险。

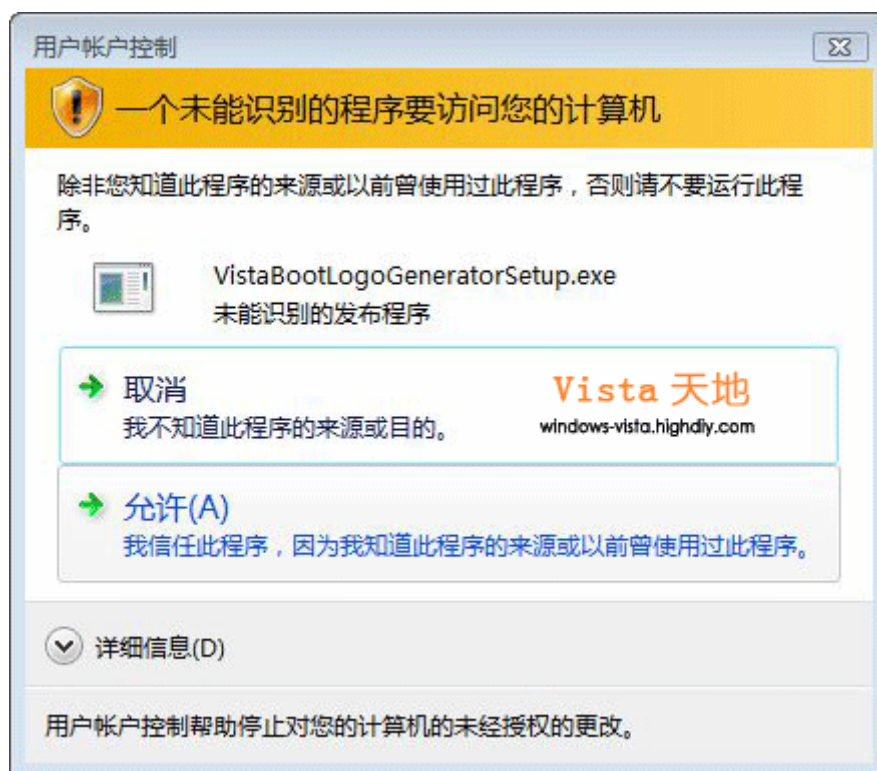
3.4 安装程序、下载文件与 **UAC**

UAC 不仅存在于系统设置的相关操作中，事实上，当我们在 Windows Vista 安装应用程序时也会经常遇到 **UAC**，特别是对通过网络下载的应用程序安装文件而言。

下图即为在撰写[定制Windows Vista启动画面](#)一文时我们所使用的Vista Boot Logo Generator下载文件，注意其图标中的小盾牌。



当 Windows Vista 检测到相应程序在安装中可能会更改系统设置时，即会弹出相应的 **UAC** 要求确认或提升权限。



3.5 更改 UAC 的提示方式

不可讳言, 频繁弹出的 UAC 提示窗口在很多时候令人厌烦, 不过, 虽然 Vista 天地也曾介绍过在 Windows Vista 中禁用 UAC 的设置方法, 但为了保证系统的安全, 我们强烈建议用户不要这么做。如果因某种原因不得不这么做, 请务必全面权衡这样做带来的风险, 以及时刻谨记禁用 UAC 的后果。

作为一种替代的解决方案, 我们可以尝试更改 UAC(用户帐户控制)消息的提示方式, 以尽可能避免操作被 UAC 弹出打断的情况。

注: 对一般用户来说, 这仍是不建议采用的方式, 因此, 除非您确知这样做存在的风险并明白如何规避, 不然请勿进行修改。

要更改 UAC 提示信息的显示方式, 首先需以本地管理员组成员身份登录——或以标准用户身份登录后提供管理员组成员的认证凭据——修改相应的安全策略。

- 在开始菜单搜索框中输入“gpedit.msc”后按回车，打开组策略对象编辑器，依次选择“计算机配置” => “Windows 设置” => “安全设置” => “本地策略” => “安全选项”；

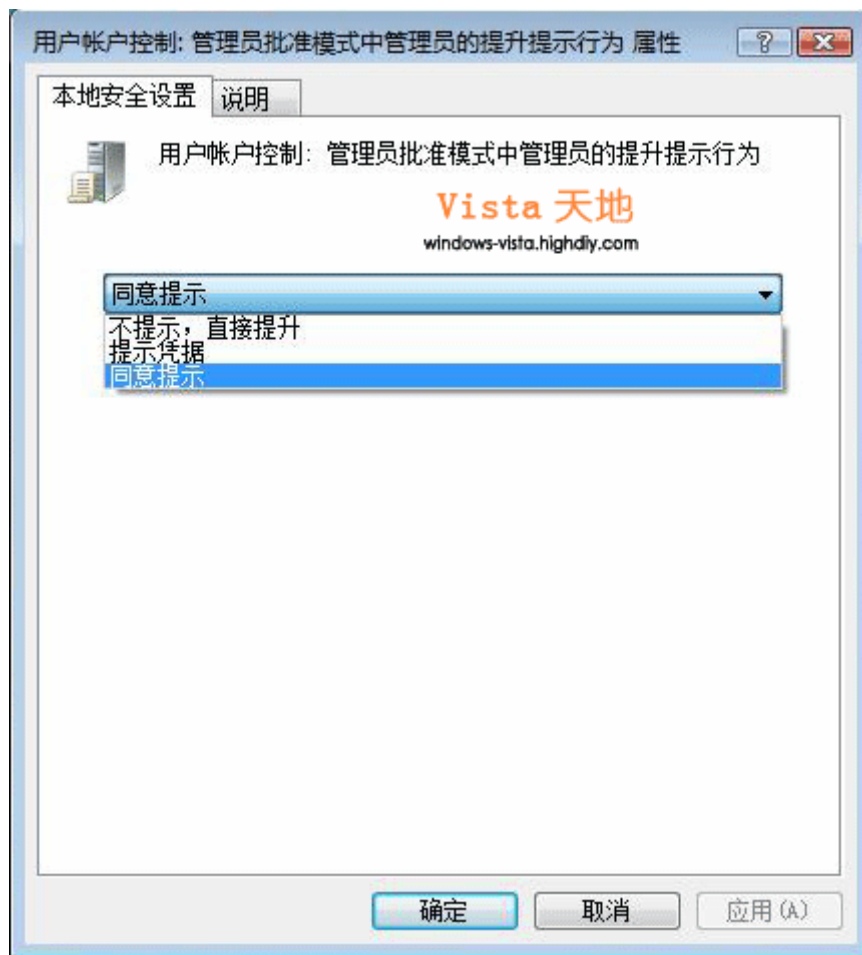
或

在开始菜单搜索框中输入“Secpol.msc”后按回车，打开本地安全策略编辑器，依次选择“本地策略” => “安全选项”；

在 Windows Vista 默认配置中，运行这两款系统设置工具均会弹出 UAC 权限信息窗口，需要用户确认。

- 更改使用管理员身份登录时 UAC 信息提示方式**

在右侧窗格中找到“用户帐户控制：管理员批准模式中管理员的提升提示行为”，双击打开，在下拉菜单中选择。



下拉菜单中共有三个选项，分别为：

- 不提示，直接提升

启用该项时，所有已标记为管理员应用程序的应用程序以及被检测出是安装应用程序的应用程序，都将使用完全管理员访问令牌自动运行。——也即是说，当使用具有管理员身份用户登录 Windows Vista 后，由系统自动处理提升权限的操作，而不会出现 UAC 确认窗口。——而所有其他应用程序都将使用标准用户令牌自动运行。

- 提示凭据

启用该项时，当需要提升权限时，用户必须输入管理员凭据。此项设置一般用于域环境或企业策略。

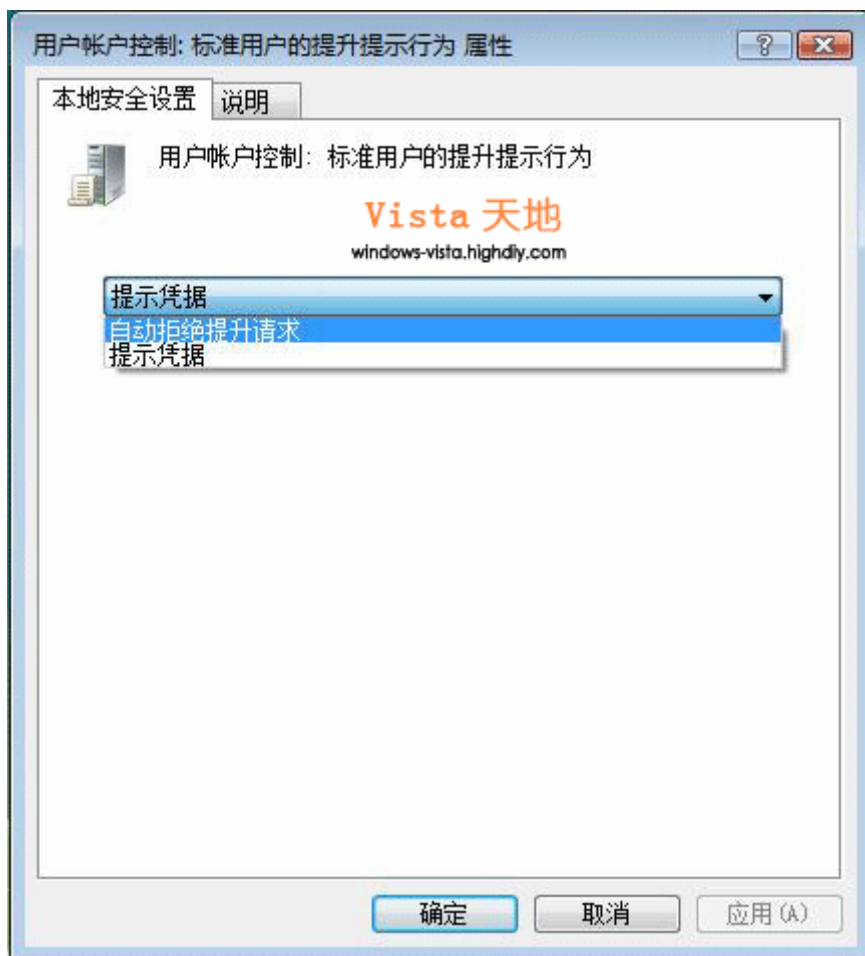
- 同意提示

该项为 Windows Vista 默认设置。

因此，如果我们选择“不提示，直接提升”项，当以管理员身份登录 Windows Vista 后，将不再看到烦人的 UAC 信息提示窗口。

- **更改使用标准用户身份登录时 UAC 信息提示方式**

在右侧窗格中找到“用户帐户控制：标准用户的提升提示行为”，双击打开，在下拉菜单中选择。



下拉菜单中共有二个选项，分别为：

- 自动阻止提升请求
启用该项后，Windows Vista 将禁止标准用户运行管理员应用程序或服务，用户只会看到来自该应用程序的错误消息，提示某个策略已经阻止运行该应用程序。
- 提示凭据
该项为 Windows Vista 默认设置。即对标准用户而言，在运行某些需要更改系统设置的程序时允许其获得管理员访问令牌——当然，前提是用户必须输入管理员凭据。

如果我们根本不想让标准用户更改系统设置，那么可直接启用“自动阻止提升请求”，这样既避免了标准用户的操作可能对系统带来的风险，同时也不会出现频繁的 UAC 提示窗口。

- 设置完毕后单击“应用”即可。

阅读更多Windows Vista使用教程及Windows Vista安装、使用技巧, 请
至[Vista天地](#)