 在Windows7操作系统中，提出了一个新的计算机安全管理机制，即UAC(用户帐户控制)。这个功能到底有什么用呢?简单的说，就是其他用户对操作系统做了更改，而这些更改需要有管理员权限的，此时操作系统就会自动通知管理员，让其判断是否允许采用这个更改。虽然在以前的版本中，也有这方面的限制。但是在Windows7中有了很大的改善。其不但对细分了控制的级别，而且还会自动通知管理员。 一、管理员根据需要可以选择不同的控制级别 在Windows7 中，将这个控制级别分为四个级别。最高的级别是“ 始终通知我 ”，即用户安装应用软件或者对应用软件进行升级、应用软件在用户知情或者不知情的情况下对操作系统进行更改、修改Windows设置等等，都会向系统管理员汇报。 第二个级别为“ 仅在应用程序试图尝试改变计算机时 ”通知系统管理员。这个级别是操作系统的默认控制级别。他与第一个级别的主要差异就在于改变Windows设置时不会通知系统管理员。在这个级别下，即使操作系统上有恶意程序在运行，也不会给操作系统造成多大的负面影响。因为其恶意程序不能够在系统管理员不知情的情况下修改系统的配置，如更改注册表、更改IE浏览器的默认页面、更改服务启动列表等等。为此对于大部分用户来说，特别是企业用户来说，这个安全级别已经够用。级别太高的话，就太过于死板了。可能系统管理员要不断的为此奔忙了。 第三个级别与第四个级别其安全性逐渐降低，最后到所

有都不通知为止。其实这个控制级别跟原先IE浏览器的控制级别类似，都是微软自定义的控制级别。作为系统管理员需要了解各个级别控制的具体内容，然后根据企业的实际情况，来设置安全级别。通常来说，安全级别越高，操作系统越安全。但是系统管理员可能需要抽出更多的时间来应对用户的抱怨。因为可能用户对操作系统任何的更改都需要告知系统管理员。鱼与熊掌不可兼得，系统管理员需要在安全与便利性上取得一个均衡。 二、用户权利不够如何通知系统管理员 不知道各位读者有没有用过微软或者其他公司的工作流产品?其实微软在这个问题的处理上就是借鉴了工作流得处理方法。当用户试图更改某个设置或者安全某个应用程序，当其权限不够时，系统就会向管理者发送一个请求。当系统管理员下次登陆系统时就会看到一个对话框。在对话框中显示了用户需要更改的设置或者要安装的应用程序。系统管理员要仔细查看这些信息，以判断是否会破坏系统的稳定性。然后可以通过这个对话框告诉操作系统，允许或者拒绝用户的更改操作。最后，系统会把系统管理员的这个决定反馈给用户。用户就可以继续后续的操作了。如果系统管理员同意的话，就可以安装应用程序或者更改操走系统的配置。显然，这个流程的话大家非常的熟悉。不错，这就是一个工作流处理流程。在Windows7操作系统中，很多地方都可以看到这个工作流的身影。这也是 Windows7 操作系统人性化的体现。 三、关掉UAC控制 如果用户不喜欢这个先进的东西，而是喜欢Window的控制方案，这也是可以的。系统管理员只需要将这个级别调到第四个级别，即关掉UAC控制。此时，跟以前的操作系统版本一样，任何的改变不会告知系统管理员。如

当用户以管理员的身份登陆到操作系统中，则应用程序对操作系统所作的任何更改都将不会提醒管理员，而是直接应用了相关的更改。 可见，此时如果是一些恶意的程序在进行更改，则会在神不知鬼不觉的情况下，更改了系统的某些设置，如网页、注册表等等。如果用户是以普通标准用户登录操作系统的，如果其所作的操作，包括安装或者升级应用程序、更改操作系统配置等等，只要其没有相关的权限，则操作系统就会直接拒绝掉。也就是，不会采用工作流的形式去通知管理员。如果用户确实有这个需要的话，只有口头去通知，并让系统管理员调整相关的权限。当系统管理员将这个UAC控制从高级别调到这第四个级别，必须重新启动后这个控制级别才会生效。 当系统管理员关闭这个UAC的话，就必须要小心各种应用程序可能对操作系统所造成的破坏，因为应用程序只要以管理员帐户运行，则其就可以访问或者修改那些受保护的区域、用户的私人数据等等。也就是说，其应用程序的权限就跟系统管理员的权限相同。另外一些恶意程序也可以在系统管理员不知情的情况下跟网络中的其他电脑、甚至互联网上的主机进行通信与数据传输，以达到破坏的作用。 其实这个UAC控制级别，在某方面看起来跟操作系统的个人防火墙比较类似。当任何应用程序有修改操作系统配置的行为(更改IE主页、修改注册表、把某个服务设置为自动启动)，都会向用户提示。当应用程序要向互联网发送信息时，也会告知用户。为此如果系统管理员用不惯这个功能，需要关闭它的话，最好能够采用其他的安全措施来替代。如可以利用这个个人防火墙来代替UAC控制级别。虽然其不能够实现UAC的所有功能，但是一些核心的保护功能个人防火

墙已经可以胜任。确实，如果企业现在已经部署了个人防火墙，那么在推广Windows7操作系统的时候，如果再采用这个UAC控制的话，就重复了。反而可能会造成用户的反感。总之，系统管理员要根据自己与用户的操作系统，在这两个方案中选择一个即可。多了反而是累赘。 四、通过域安全策略来统一这个管理级别 企业中的客户端数量往往不在少数。一个系统管理员管理的客户端没有几百台的话，也有几十台。如果一一的去调整这个UAC的控制级别，显然是一项重复、无挑战性的工作。根据笔者的测试，其实这个UAC控制级别可以跟组策略或者域安全策略结合使用。即可以在域控制器级别上或者组级别上设置这个级别。然后当客户端加入到这个域或者这个组的话，就会继承这个管理级别。也就是说，不需要在各个客户端上再进行一一配置。说实话，微软在这方面一直都做的不错。虽然微软的域环境搭建与管理起来是复杂一点，但是其功能还是比较强大的。如果要让Windows操作系统的一些高级功能应用的更加顺手，则这个域环境往往是少不了的。至少这个域环境能够提供一个统一管理各个客户端的平台。 编辑特别推荐: 微软WindowsServer2008认证体系介绍 MCSE认证考试全程心得 联想与微软首推Windows7联想“ EE ”认证 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