

24 January 2007

By: Marius Oiaga, Technology News Editor



[Admin Approval Mode in Windows Vista](#)

A feature of the UAC

The admin approval mode in Windows Vista illustrates how the security features of the operating system have evolved beyond Windows XP. The administrator approval mode is active by default for all the users that are members of the local administrator group. With the introduction of the User Account Control in Windows Vista, Microsoft has labored to deliver a balance between security via privilege limitations and functionality. In Windows XP, a standard user found that the actions they were able to perform were confined to the point of lost functionality. This is also one of the reasons why in Windows XP, standard user accounts are less than popular. In this aspect, the security delivered by limiting the administrator privileges was traded off for complete functionality. In Windows Vista, Microsoft has integrated a common denominator in the UAC settings: the admin approval mode. "In this mode (which is on by default for all members of the local administrators group), every user with administrator privileges runs normally as a standard user; but when an application or the system needs to do something that requires administrator permissions, the user is prompted to approve the task explicitly. Unlike the "super user on" function from UNIX that leaves the process elevated until the user explicitly turns it off, admin approval mode enables administrator privileges for just the task that was approved, automatically returning the user to standard user when the task is completed," explained Jim Allchin, Microsoft Co-President, Platform and Services Division. Allchin went on to explain that the functionality is simply a convenience feature designed for administrators. The admin approval mode does not create a security boundary between processes. In this context, in the absence of process isolation, interference is possible. "If an administrator performs multiple tasks on the same desktop, then malware may potentially be able to inject or interfere with an elevated process from a non-elevated process. Thus, the most secure configuration for Windows Vista is to run processes in two separate accounts, with only administrator tasks performed using an administrator account and all other tasks performed under the standard user account," added Allchin.