

User Account Control (UAC), già noto come User Account Protection o Least User Access, è un nuovo set di tecnologie di infrastruttura che consentono una migliore gestione del desktop riducendo nel contempo l'impatto dei malware sul sistema. Se la funzionalità è attivata in Windows (<http://www.tweakness.net/topic.php?id=2951#>) Vista, tutti gli utenti, inclusi gli amministratori, accedono con un account utente standard. Agli amministratori è consentito avviare selettivamente applicazioni amministrative in grado di utilizzare i privilegi completi dell'account solo quando è necessario. Quando gli utenti con privilegi accedono al proprio account, in realtà accedono all'ambiente di un account utente standard, ma possono eseguire applicazioni con i propri privilegi completi previa approvazione. Di default, le attuali versioni di Windows configurano la maggior parte degli account utente come membri del gruppo di amministratori. Questo costituisce un serio rischio di sicurezza perché i malware writer riescono più facilmente a guadagnare il controllo completo dei sistemi attaccati. Con la funzionalità UAC, Vista separa i privilegi e le attività dell'utente standard da quelli amministrativi, riducendo enormemente la superficie d'attacco.

Tuttavia, durante le fasi di test del sistema, UAC è stato molto criticato dai tester. In particolare in Vista Beta 2 (<http://www.tweakness.net/topic.php?id=2303>) la funzione di sicurezza richiedeva all'utente di cliccare su numerose (troppe) richieste di permesso prima di poter effettuare operazioni anche comuni. Microsoft (<http://www.tweakness.net/topic.php?id=2951#>) ha carpito il feedback e in RC1 ha introdotto molti miglioramenti (<http://www.tweakness.net/topic.php?id=2558>) per la tecnologia (<http://www.tweakness.net/topic.php?id=2951#>) proprio nel tentativo di renderla meno "petulante". Il colosso ha implementato anche i cosiddetti "shim di compatibilità", correzioni per gli applicativi esistenti che non vengono eseguiti correttamente sotto Standard User.

Ci sono due modi principali per disattivare UAC: La soluzione più facile è quella di sfruttare il Pannello di Controllo. Digitate "UAC" nella barra di ricerca nella parte alta della finestra e verrà mostrata come task (dovrete essere nella Home del Pannello (<http://www.tweakness.net/topic.php?id=2951#>) e non in Classic View) la possibilità di disattivare UAC in pochi click (riavvio necessario). Questo facile metodo è drastico, cioè disattiva in toto le funzionalità UAC. Esiste però un metodo più raffinato che preserverà alcuni dei benefici di UAC eliminando nel contempo tutte le "fastidiose" richieste di elevazione. Dovrete modificare i criteri di sicurezza locali: dalla barra di ricerca in Start, digitate "Local Security Policy", accettate quest'ultimo "elevation prompt", dallo snap-in selezionate Security Settings -> Local Policy -> Security Options e scorrete in fondo, dove troverete 9 diverse impostazioni per il fine-tune della configurazione di UAC. La scelta migliore è probabilmente quella di modificare la voce "User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode" da "Prompt for consent" a "Elevate without prompting".

Con questo secondo metodo, a dispetto del Windows Security Center che notificherà ugualmente la mancanza di UAC, la tecnologia di protezione non sarà del tutto disattiva. Tutti i processi continueranno ad eseguirsi in modalità standard user. Verificalo aprendo un prompt dei comandi e provando a salvare un file in C:\. Riceverete un messaggio di errore. Viceversa quando un processo è segnato per richiedere una elevazione di privilegio, non sarà attivato il prompt in secure desktop o meglio la richiesta sarà accettata in maniera silente. Per verificarlo cliccate col tasto destro del mouse su un link ad un prompt di comando e scegliete "Run as Administrator". Il prompt si aprirà senza richiesta di elevazione, e il titolo della finestra mostrerà che state agendo con pieni privilegi di amministratore.