What is User Account Control?

TN technet.microsoft.com/en-us/library/dd835562(v=ws.10).aspx

The most important rule for controlling access to resources is to provide the least amount of access privileges required for a user to perform his or her necessary tasks. Many tasks do not require administrator privileges. However, because versions of Windows earlier than Windows Vista created all user accounts as administrators by default, users logged on to their computers with an administrator account. Without User Account Control (UAC), when a user is logged on as an administrator, that user is automatically granted full access to all system resources.

However, most users do not require such a high level of access to the computer. Often users are unaware that they are logged on as an administrator when they browse the Web, check e-mail, and run software. While logging on with an administrator account enables a user to install legitimate software, the user can also unintentionally or intentionally install a malicious program. A malicious program installed by an administrator can fully compromise the computer and affect all users. Because UAC requires an administrator to approve application installations, unauthorized applications cannot be installed automatically or without the explicit consent of an administrator.

Because UAC enables users to easily run as standard users:

- IT departments can have more confidence in the integrity of their environments, including system files, audit logs, and system-wide settings.
- Administrators no longer need to devote large amounts of time to authorizing tasks on individual computers. This allows administrators to spend more time on overall system maintenance, reducing an organization's total cost of ownership for its enterprise software platform.
- IT administrators gain better control over software licensing because they can ensure that only authorized applications are installed. As a result, they will no longer have to worry about unlicensed or malicious software endangering their network, causing system downtime and data loss, or creating licensing liabilities.

Definitions

Access token. When a user logs on to a computer, the system creates an access token for that user. The access token contains information about the level of access that the user is granted, including specific security identifiers (SIDs) and Windows privileges.

Admin Approval Mode. When the user runs applications that perform administrative tasks (administrator applications), the user is prompted to change or "elevate" the security context from a standard user to an administrator, called Admin Approval Mode. In this mode, the administrator must provide approval for applications to run on the secure desktop with administrative privileges.

Consent prompt. The consent prompt is presented when a user attempts to perform a task that requires a user's administrative access token. The user provides consent by clicking **Yes** or denies consent by clicking **No**.

Credential prompt. The credential prompt is presented when a standard user attempts to perform a task that requires a user's administrative access token. The user provides the user name and password for an account that is a member of the local administrators group.