12.5.8 UAC Facts

User Account Control (UAC) helps minimize the dangers of unwanted actions or unintended software installations. UAC prompts for permission before allowing changes that can affect your computer's security or performance. How UAC works depends on the user account type:

- A standard user account is an account that has the least amount of user rights and privileges required to perform most basic tasks. An administrator account can perform any action on the system.
- Regardless of the user account type, the system first attempts to perform any action using standard user privileges. If standard user rights are not sufficient to perform a task, UAC requests privilege *elevation*:
    - The standard user is prompted to provide administrator user credentials (username and password). This process is referred to as *Prompt for credentials*.
    - The administrator user is asked whether the requested task should be allowed. Because the administrator has already logged on with an administrator username and password, this is a simple Continue or Cancel question. This process is referred to as *Prompt for consent*.
- Actions that require elevated credentials are typically indicated in the interface with a shield icon.
- Prompting for credentials or consent activates the Secure Desktop. With the Secure Desktop, the desktop and all active applications are darkened, and the prompt appears over the shaded desktop. You must respond to the prompt before you can continue with the requested operation or return to the desktop.
- If you disable the Secure Desktop, the prompt is still shown, but the desktop is not dimmed (or locked), allowing you to work with the desktop without responding to the prompt.

To manage UAC settings go to Control Panel and follow these steps:

1. Select **System and Security**.
2. Select **Security and Maintenance**.
3. Expand **Security**.
4. Go to User Account Control, select **Change Settings**.

You can use the slider displayed to select one of the following UAC configurations:

Setting	Description
Always notify	When configured to always notify: - Notification occurs when programs make changes - Notification occurs when you make changes - The desktop is dimmed (Secure Desktop is enabled)
Notify me only when apps try to make changes to my computer (default)	When configured to notify for program changes: - Notification occurs when programs make changes - Notification does not occur when you make changes - The desktop is dimmed (Secure Desktop is enabled) This is the default setting.
Notify me only when apps try to make changes to my computer (do not dim my desktop)	When configured to notify for program changes without dimming the desktop: - Notification occurs when programs make changes - Notification does not occur when you make changes - The desktop is not dimmed (Secure Desktop is disabled) This setting is recommended only if it takes a long time to dim the desktop.
Never notify	When configured to never notify, UAC is disabled. No notification occurs and the Secure Desktop is disabled. This setting is not recommended.

Additional control over how UAC functions can be configured under Local Security Policy settings by following these steps:

1. In the search box, type **secpol.msc**.
2. Expand **Local Policies**.
3. Select **Security Options**.

You can configure the following Local Security Policies:

- Use Admin Approval Mode for the built-in Administrator account
- Allow UIAccess applications to prompt for elevation without using the secure desktop

- Behavior of the elevation prompt for administrators in Admin Approval Mode
- Behavior of the elevation prompt for standard users
- Detect application installations and prompt for elevation
- Only elevate executable files that are signed and validated
- Only elevate UIAccess applications that are installed in secure locations
- Run all administrators in Admin Approval Mode
- Switch to the secure desktop when prompting for elevation

If you disable UAC (or configure UAC to Never notify), the system no longer prompts when you or a program makes changes that require administrative privileges. This is not a secure configuration, and could expose your computer to attacks. If you disable the UAC prompts, you should be careful about programs that you run because they'll have the same access to your computer as you do.

After enabling or disabling UAC, you must restart the computer to apply the changes. Other changes (such as changing the prompt behavior) can be applied without restarting.