User Account Control (UAC) in Windows 10 and 11

Introduction to User Account Control (UAC)

User Account Control (UAC) is a security feature in Microsoft Windows 10 and Windows 11 that helps prevent unauthorized changes to the operating system. It is designed to protect computers from potentially harmful applications, malicious software, and unintended administrative actions.

UAC works by notifying users whenever an application or process attempts to perform an operation that requires administrative privileges. Depending on the system configuration and the type of operation, Windows may display a confirmation prompt asking the user to approve or deny the action.

The primary purpose of UAC is to ensure that applications do not automatically receive elevated administrative permissions simply because a user is logged on with an administrator account.

UAC is an important component of the Windows security architecture and supports the principle of least privilege, which means that users and applications should operate with only the permissions necessary to perform their tasks.

Benefits and purpose

UAC was introduced to reduce the risks associated with running Windows applications with unrestricted administrative privileges.

Its main objectives include:

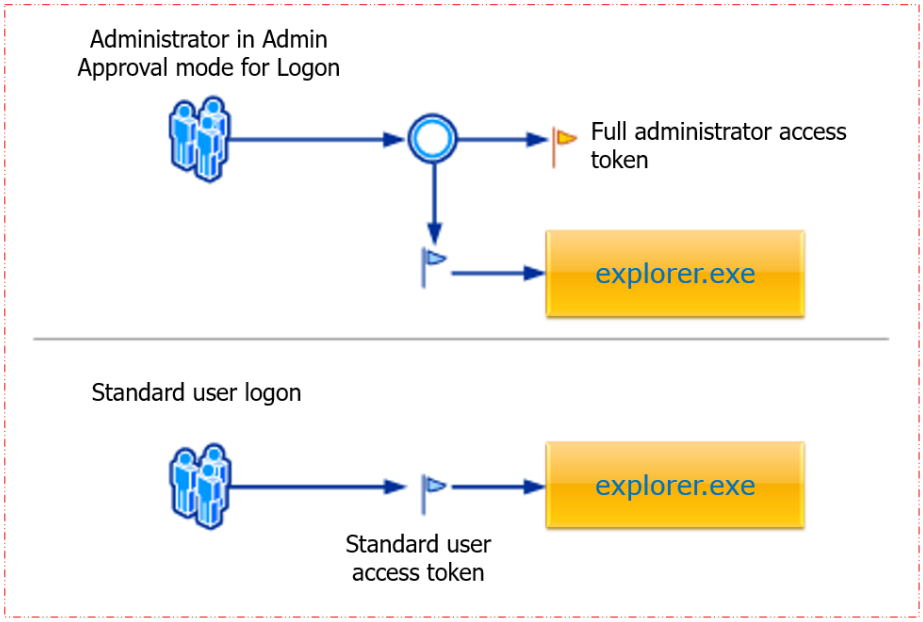
- Prevent unauthorized system changes: Require approval before applications perform certain administrative operations.
- Reduce malware impact: Help prevent malicious applications from silently modifying protected system resources.
- Protect system configuration: Restrict unauthorized changes to Windows settings, system files, and registry locations.
- Promote least-privilege operation: Allow users to perform everyday activities without continuously operating with elevated permissions.
- Improve user awareness: Inform users when an application requests administrative privileges.

UAC does not guarantee complete protection against malware. Instead, it provides an additional security layer that works alongside Microsoft Defender Antivirus, Windows Firewall, application control, and other Windows security mechanisms.

How UAC works

UAC uses a mechanism called *Admin Approval Mode* to control how administrative privileges are granted.

When a user signs in to Windows, the operating system determines the user's account type and creates the appropriate access tokens.



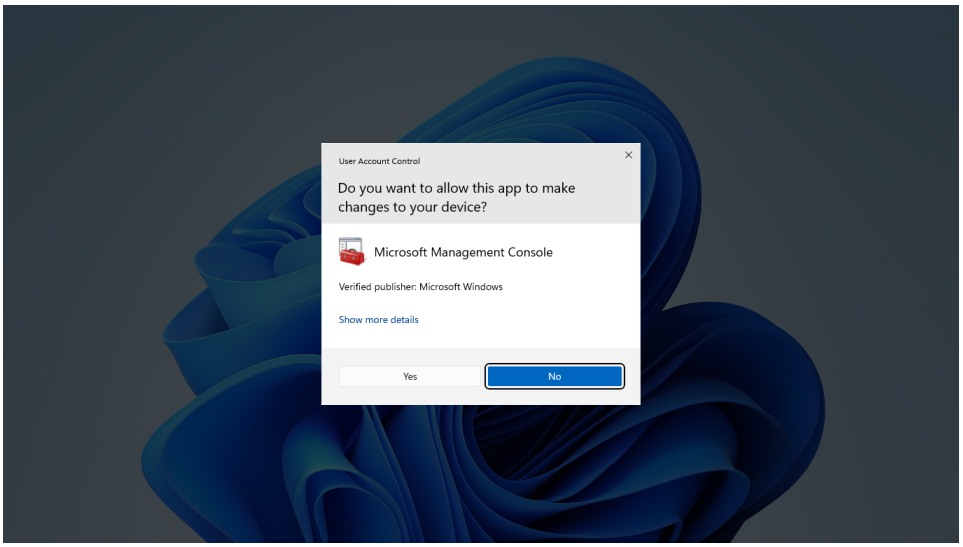
For standard users, applications normally run with standard user permissions.

For administrators operating with Admin Approval Mode enabled, Windows generally creates two access tokens:

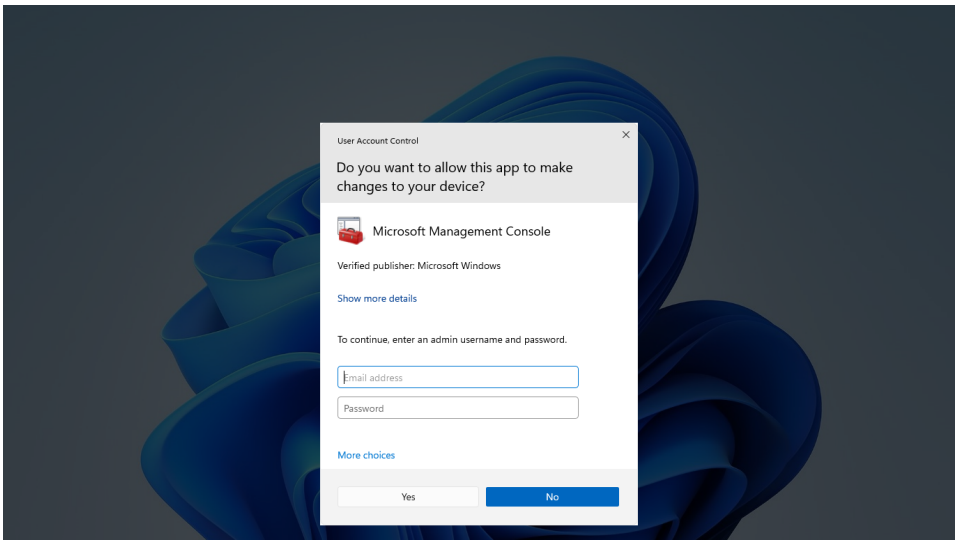
1. **Standard user token:** Used for normal application execution and everyday activities.
2. **Elevated administrator token:** Contains administrative privileges and is used only when an operation requires elevation.

When an application attempts to perform an administrative operation, Windows checks whether elevation is required.

If elevation is required, Windows displays a UAC prompt. The user must provide the appropriate approval or administrator credentials before the process can continue.



The credential prompt is presented when a standard user attempts to perform a task that requires a user's administrative access token. Administrators can also be required to provide their credentials by setting the User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode policy setting value to Prompt for credentials.



UAC Notification levels

Windows 10 and Windows 11 provide a graphical interface for configuring UAC notification behavior. The notification settings contain four levels.

Level	Description
Always notify	Windows notifies the user whenever applications attempt to install software or make changes to the computer, and when the user makes changes to Windows settings.
Notify me only when apps try to make changes *(default)*	Windows notifies the user when applications attempt to make changes but does not notify when the user makes changes to Windows settings.

Notify me only when apps try to make changes *(do not dim my desktop)*	Similar to the previous level, but the UAC prompt appears on the normal desktop instead of switching to the Secure Desktop.
Never notify	Windows does not display standard UAC notifications. This significantly reduces protection against unauthorized administrative changes.

About this article

- Written by Gary Phatt, a TheOpenRoad Support employee.
- Still need help? Please write to us in the comment section below or contact TheOpenRoad support.

TheOpenRoad™

Please rate your experience with this article today:

When you select a number, *1 being the lowest and 9 being the highest*; the page will refresh and your feedback will be submitted to TheOpenRoad.

1 2 3 4 5 6 7 8 9

Revision #2
Created 2026-10-30 05:20:42 UTC by Gary Phatt
Updated 2026-10-30 05:53:03 UTC by Gary Phatt