

By Deb Shinder, MCSE, MVP

One of the most talked about new features in Windows Vista is the User Account Control (UAC) security mechanism, which has gone through several names/acronyms (Limited User Account/LUA, User Account Protection/UAP) before settling into its present incarnation. Here's a look at why UAC is needed, how it works, and how you can make it a little less annoying in everyday use.

The need for UAC

UAC addresses the problem of users routinely logging on as administrators--something that many users (including IT pros who theoretically know better) do as a matter of course because administrative privileges are required to perform so many tasks. Microsoft tried to address this in previous operating systems by providing the secondary logon feature ("run as"), but most users continued to run their systems as local administrators.

So what's the problem with running as an administrator all the time? It presents a security risk, especially if the computer is infected with malicious software that can run at the privilege level of the logged-on user. If the user is logged on with an admin account, the malware has free rein. But the traditional cure is almost as bad as the disease: If you force users to log on with regular user accounts, they may be unable to perform many necessary tasks, and some applications won't run properly.

Vista addresses the problem in a couple of ways. Common tasks, such as installing a printer driver, creating a VPN connection, or installing critical Windows updates, will no longer require administrative privileges. UAC takes it even further: Now, even if you log on with an administrative account, you'll still be running most applications in standard user mode unless and until you try to perform tasks that require the elevated privileges.

How UAC works

A stated goal of UAC is to separate those tasks that truly require administrative privileges from "standard" tasks, so that users can run with standard user privileges except when it's absolutely necessary to elevate privileges.

The logon process has been changed under the hood. When you log on with an administrative account, you get both a full administrator access token and a standard user access token. The standard user token is used to launch Explorer.exe (the parent process of all other user-initiated processes; those processes inherit their access token from Explorer.exe). That means all applications will run with that standard user token unless privileges are elevated by responding to the UAC prompt. This description assumes that administrative accounts are configured to run in Administrator Approval Mode.

Administrator Approval Mode is the mechanism that protects against malicious software attacks when you're logged on as an administrator. In this mode, you still run with standard privileges unless/until a program needs administrative privileges to accomplish a task. Then, a dialog box asks for your permission to continue the action, as shown in **Figure A**.

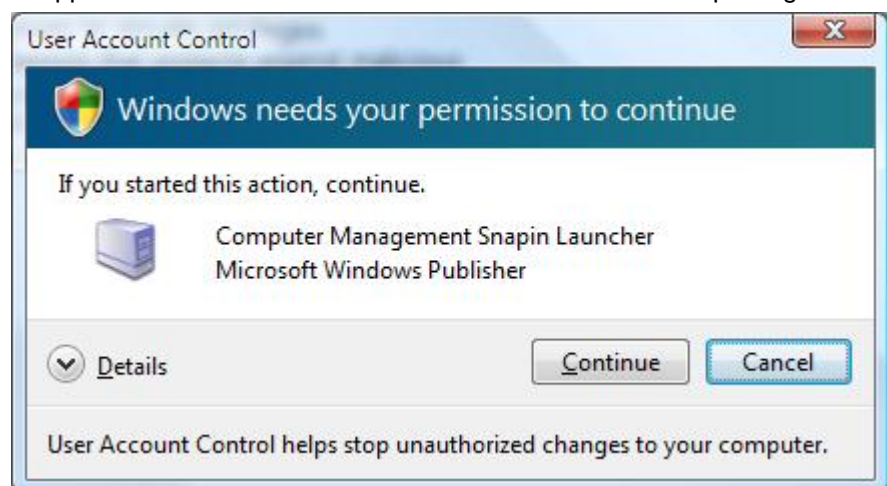


Figure A: If you try to perform a task requiring administrative privileges while logged on with an admin account, you're asked for permission to continue.

Tip

Although UAC will help protect against the exploitation of elevated privileges by malware, you should still be sure to run antivirus and anti-spyware programs and ensure that they're regularly updated.

However, this is not as secure as logging on with a standard user account. When you're logged on as a regular user, the dialog box will require that you type in administrative credentials to continue. It's easy for administrators to get in the habit of just clicking the Continue button without taking the time to consider the implications, negating the usefulness of this feature.

Vista makes it easier to tell what actions require administrative privileges by identifying them with a shield icon on the buttons for backing up files or backing up the computer (**Figure B**). Note that restoration buttons don't require administrative privileges.



Figure B: A shield icon identifies tasks that require administrative privileges.

Once upon a time, we had the Power Users group to allow more experienced users to do things like install printers and programs. With UAC, there's no need for the Power User mode, but it's still available for backward compatibility with previous versions of Windows. If you want to use the Power Users group on Vista, you need to apply a security template that changes the default permissions on the registry and system folders so that they'll be the same as with Windows XP.

There's also no need for administrators to switch back and forth between a regular user account and admin account frequently, either by logging off and back on with a different account or by using the Run As command, since Admin Approval Mode de-elevates your admin privileges when you're performing routine tasks.

By default, when a UAC dialog box appears prompting you for permission to continue, the rest of the desktop goes dark and won't respond to input. This feature is called Secure Desktop Mode, and it prevents other software (such as malware running on the machine without the user's knowledge) from interacting with the prompt.

Configuring UAC behavior

IT administrators can configure how UAC behaves by editing the local security policy or domain-based group policies. For example, if you don't want administrator accounts to run in Admin Approval Mode (that is, you don't want to be prompted every time you need elevated privileges), you can turn off that feature. You can also configure group policy to limit standard users to installing only approved applications and devices.

You'll find the UAC policy settings under the Local Policies | Security Options section of the local security policy, as shown in **Figure C**.

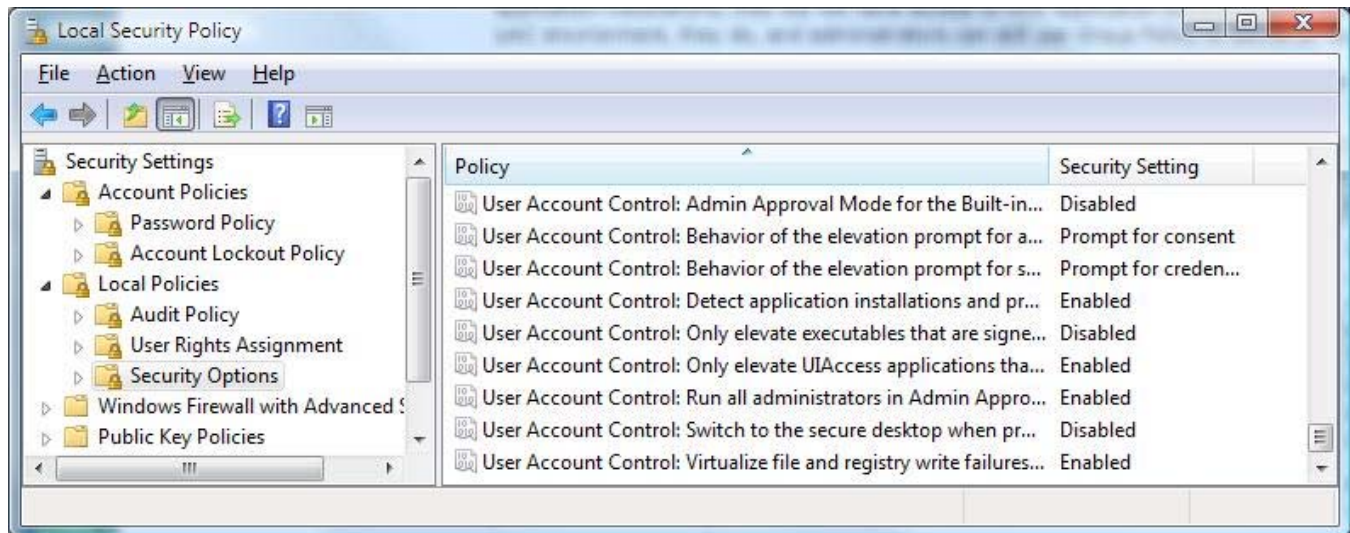


Figure C: Administrators can control the behavior of UAC by editing the local security policy or domain group policy.

Here are the various policy settings you can configure:

- **Admin Approval Mode For The Built-in Administrator Account:** This setting is disabled by default for new installations and for upgrades where the built-in account isn't the only administrator account active on the machine. If you enable it, the built-in admin account will run in Admin Approval Mode, which means it runs in standard user mode for routine operations and prompt for permission when elevated privileges are needed.
- **Behavior Of The Elevation Prompt For Administrators In Admin Approval Mode:** The default setting is to prompt administrators for permission to elevate privileges. You can change this to No Prompt, in which case elevation of privileges happens automatically when needed to perform a task. This negates the extra security provided by UAC when logged on with an administrative account, and it's not recommended under normal circumstances--although many administrators will probably use this setting to avoid the annoying pop-up of the UAC dialog box. Alternatively, you can increase security even more by setting this policy to prompt for credentials instead of just permission. Then, you'll have to enter an administrator password before privileges will be elevated, even though you're already logged on as an administrator.
- **Behavior Of The Elevation Prompt For Standard Users:** The default for this policy depends on the environment. Home users will be prompted to supply administrative credentials if needed to perform a task. In the enterprise, no prompt is presented. The user gets a dialog box explaining that he/she doesn't have the proper privileges to perform this task. The only way to do so is to log off and log back on with an administrative account or use the Run As command to enter administrative credentials. You can change this policy to No Prompt or Prompt as you desire.
- **Detect Application Installations And Prompt For Elevation:** When this policy is enabled, whenever an installer program tries to run, the user is prompted for permission (if logged on as an administrator) or to enter credentials (if logged on as a regular user). If it's disabled, users will not be able to install programs. By default, the policy is enabled for home users and disabled for enterprise users.
- **Only Elevate Executables That Are Signed And Validated:** This policy is disabled by default, which means both signed and unsigned executable files will run. To increase security in an enterprise environment, you can

enable the policy so that a check of the certificate is required whenever an application requests elevation of privileges.

- **Only Elevate UIAccess Applications That Are Installed In Secure Locations:** This policy is enabled by default, so that the system will not give UIAccess privileges and user rights to any executable files that are launched from a location other than the Program Files or Windows directories. The access control lists on these two directories prevent users from being able to modify files contained in them. If a UIAccess executable program is launched from any other directory, it launches without additional privileges. When you disable this policy, Vista does not check the location, which means any UIAccess application that's launched will run with the user's full access privileges (after the user approves running the program).
- **Run All Administrators In Admin Approval Mode:** This policy is enabled by default, which means administrators will always be prompted (according to the policy settings for Behavior Of The Elevation Prompt For Administrators In Admin Approval Mode, as discussed above). If you disable this policy, the Application Information Service (AIS) won't start automatically, so UAC is effectively turned off. You have to reboot the computer to make changes to this policy effective. If you turn off UAC in this way, upon reboot you'll receive a dialog box informing you that the security of the operating system has been reduced and giving you the option of re-enabling it. If you don't want administrators to be prompted, the better way to accomplish this is via the Behavior Of The Elevation Prompt For Administrators In Admin Approval Mode policy.
- **Switch To The Secure Desktop When Prompting For Elevation:** This policy is enabled by default but will probably be disabled by many administrators who dislike having the desktop go dark when they're asked for permission to continue an operation. When it's enabled, the desktop can receive messages only from Windows processes. No other software can interact with it. If you disable it, the UAC prompt will still be displayed (assuming you haven't disabled it with previously discussed policies), but it will be displayed on the user's interactive desktop.
- **Virtualize File And Registry Write Failures To Per-User Locations:** This policy is enabled by default, which means write failures for pre-Vista applications (those that are not UAC compliant) are redirected to defined locations in the file system and registry. If you disable this policy, any non-UAC compliant applications that try to write to the Program Files, Windows, or System 32 directories will fail.

What if you have pre-Vista applications?

If you need to run legacy applications that were not designed to be compliant with UAC, you may need to configure them to work with Vista. If a program must be able to perform administrative tasks, it has to be marked with a requested execution level to prompt users for approval before running with administrative privileges.

You can mark applications to run with any of three requested execution levels:

- **RunAsInvoker:** The application runs with the same privileges and rights as the parent process that launches it (usually this is Explorer.exe, which runs as a standard user application).
- **RunAsHighest:** The application runs with the highest privileges and rights that the logged-on user can run. This is used for applications that can be run by both administrators and standard users with different behaviors for each or those that require privileges and rights higher than a standard user but don't require the user to be a local administrator.
- **RunAsAdmin:** The application runs only with administrative privileges. It won't run for a standard user; the logged-on user must belong to the local administrators group.

You can use the Application Compatibility Toolkit to mark programs and fix these compatibility problems. For more details, see TechNet's [Windows Application Compatibility](#) page.

Summary

User Account Control (UAC) is one of the most important new security features in Vista. It protects against malware elevation of privileges, even when someone is logged on with an administrative account. Administrators can modify UAC behavior or even turn it off (although that's not recommended) by editing the local security policy or domain group policies.


Glossary

- **Admin Approval Mode:** Default setting in which Vista runs most applications with standard user permission even when logged on with an administrative account; requires permission to elevate privileges when necessary.
- **File/registry virtualization:** A new feature that gives an application its own virtualized view of a resource it is attempting to modify.
- **Legacy applications:** Applications written pre-Vista that are not UAC compliant.
- **Secure Desktop:** The darkened desktop that appears when the UAC dialog box is open, indicating that the desktop is locked and can't be interacted with.
- **Shield icon:** Indicates that the operation performed by clicking a button marked with this icon requires administrative privileges.



Debra Littlejohn Shinder is a technology consultant, trainer and writer who has authored a number of books on computer operating systems, networking, and security. These include *Scene of the Cybercrime: Computer Forensics Handbook*, published by Syngress, and *Computer Networking Essentials*, published by Cisco Press. She is co-author, with her husband, Dr. Thomas Shinder, of *Troubleshooting Windows 2000 TCP/IP*, the best-selling *Configuring ISA Server 2000*, and *ISA Server and Beyond*.

Additional resources

- TechRepublic's [Downloads RSS Feed](#) 
- Sign up for TechRepublic's [Downloads Weekly Update](#) newsletter
- Sign up for our [Windows Vista Report](#) newsletter
- Check out all of TechRepublic's [free newsletters](#)
- ["Installing Windows Vista: The good, the bad, and the ugly"](#) (TechRepublic download)
- ["Get an in-depth look at Vista firewall's advanced configuration features"](#) (TechRepublic download)
- ["Vista's Windows Meeting Space offers enhanced functionality for real-time collaboration"](#)

Version history

Version: 1.0

Published: November 29, 2006

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team