User Account Control Step-by-Step Guide

TN technet.microsoft.com/en-us/library/cc709691(v=ws.10).aspx

User Account Control (UAC) is a security component that allows an administrator to enter credentials during a non-administrator's user session to perform occasional administrative tasks. This step-by-step guide provides the instructions that are necessary for using UAC in a test environment. You can use this guide to test how your line-of-business (LOB) applications run in Windows 7 and Windows Vista.

In this guide

This guide is intended for the following audiences:

- IT planners and analysts who are evaluating the product
- Security architects who are responsible for implementing trustworthy computing
- Administrators who need to control the behavior of UAC

This document is not intended to provide a comprehensive, detailed description of UAC. Additional resources include the following:

What is User Account Control?

User Account Control (UAC) is a security component that enables users to perform common tasks as non-administrators (called standard users in Windows Vista), and as administrators without having to switch users, log off, or use Run As. User accounts that are members of the local Administrators group run most applications as a standard user. By separating user and administrator functions, UAC helps users move toward using standard user rights by default.

When an administrator logs on to a computer that is running Windows 7 or Windows Vista, the user is assigned two separate access tokens. Access tokens, which contain a user's group membership and authorization and access control data, are used by the Windows operating system to control what resources and tasks the user can access. The access control model in earlier Windows operating systems did not include any failsafe checks to ensure that users truly wanted to perform a task that required their administrative access token. As a result, malicious software could install on users' computers without notifying the users. (This is sometimes referred to as a "silent" installation.)

Even more damaging, because the user is an administrator, the malicious software could use the administrator's access control data to infect core operating system files, and in some instances, become nearly impossible to remove.

Important

For more information about the UAC changes in Windows 7, see What's New in User Account Control.

The primary difference between a standard user and an administrator is the level of access that the user has over core, protected areas of the computer. Administrators can change the system state, turn off the firewall, configure security policies, install a service or a driver that affects every user on the computer, and install software for the entire computer. Standard users cannot perform these tasks, and they can only install per-user software.

Unlike earlier versions of Windows, when an administrator logs on to a computer running Windows 7 or Windows Vista, the user's full administrator access token is split into two access tokens: a full administrator access token and a standard user access token. During the logon process, authorization and access control components that identify an administrator are removed, resulting in a standard user access token. The standard user access token is then used to start the desktop, the Explorer.exe process. Because all applications inherit their access control data from the initial launch of the desktop, they all run as a standard user.

After an administrator logs on, the full administrator access token is not invoked until the user attempts to perform an administrative task. When a standard user logs on, only a standard user access token is created. This standard user access token is then used to start the desktop.

Important

Because the user experience can be configured with Group Policy, there can be different user experiences, depending on policy settings. The configuration choices made in your environment will affect the prompts and dialog boxes that are seen by standard users, administrators, or both.

Requirements for User Account Control

We recommend that you first use the steps provided in this guide in a test environment. Step-by-step guides are not necessarily meant to be used to deploy features in the operating system without accompanying documentation (as listed in the Additional resources section), and this guide should be used with discretion as a stand-alone document.

Setting up the test lab

The lab configuration needed for testing UAC includes a domain controller running Windows Server 2008 R2 or Windows Server 2008; a member server running Windows Server 2008 R2 or Windows Server 2008; and a client computer running Windows 7 or Windows Vista. The domain controller, member server, and the client computer should be on an isolated network, and they should be connected through a common hub or Layer 2 switch. Private addresses should be used throughout the test configuration.

Key scenarios for User Account Control

This guide covers the following scenarios for UAC:

Note

The three scenarios that are included in this guide are intended to help administrators become familiar with the UAC feature. They include the basic information and procedures that administrators need to start using UAC. Information and procedures for advanced or customized UAC configurations are not included in this guide.

Scenario 1: Request an application to run elevated one time

In Windows Vista, UAC and its Admin Approval Mode are enabled by default. When UAC is enabled, local administrator accounts run as standard user accounts. This means that when a member of the local Administrators group logs on, they run with their administrative privileges disabled. This is the case until they attempt to run an application or task that has an administrative token. When members of the local Administrators group attempt to start such an application or task, they are prompted to consent to running the application as elevated. Scenario 1 details the procedure to run an application or task as elevated one time.

Note

To perform the following procedure, you must be logged on to a client computer as a member of the local administrators group. You cannot be logged on with the computer (or built-in) administrator account because Admin Approval Mode does not apply to this account (the built-in administrator account is disabled on new installations of Windows Vista).

To request an application to run elevated one time

1. Start an application that is likely to have been assigned an administrative token, such as Microsoft Windows Disk Cleanup. A **User Account Control** prompt is displayed.
2. Verify that the details presented match the request you initiated.
3. In the **User Account Control** dialog box, click **Continue** to start the application.

Scenario 2: Configure an application to always run elevated

Scenario 2 is similar to the previous scenario in that you want to run an application or process as elevated with the administrator access token. However, in this scenario you want to run an application that has not been marked by the developer or identified by the operating system as an administrative application. Some applications, such as internal line-of-business applications, or non-Microsoft products might require administrative rights, but they have not been identified as such. In this scenario, you mark an application to prompt the user for consent, and if granted, to run as an administrative application. The following procedure steps you through this process.

Note

To perform the following procedure, you must be logged on to a client computer as a member of the local administrators group. You cannot be logged on with the computer (or built-in) administrator account because Admin Approval Mode does not apply to this account.

Important

This procedure cannot be used to prevent UAC from prompting for consent to run an administrative application.

To configure an application to always run elevated

1. Right-click an application that is not likely to have been assigned an administrative token, such as a word processing application.
2. Click **Properties**, and then select the **Compatibility** tab.
3. Under **Privilege Level**, select **Run this program as an administrator**, and then click **OK**.

Note

If the **Run this program as an administrator** option is unavailable, it means that the application is blocked from always running elevated, the application does not require administrative credentials to run, the application is part of the current version of the operating system, or you are not logged on to the computer as an administrator.

Scenario 3: Configure User Account Control

Scenario 3 outlines some common tasks that local administrators perform during the set up and configuration of client computers running Windows 7 or Windows Vista. The following procedures step you through the tasks of turning off UAC, disabling Admin Approval Mode, disabling UAC from prompting for credentials to install applications, and changing the elevation prompt behavior.

Important

Advanced configuration options for UAC are not available in Windows Vista Starter, Windows Vista Home Basic, or Windows Vista Home Premium.

Turning off UAC

Use the following procedure to disable UAC.

To perform the following procedure, you must be able to log on with or provide the credentials of a member of the local **Administrators** group.

Important

Turning off UAC reduces the security of your computer and may expose you to increased risk from malicious software. We do not recommend leaving UAC disabled.

To turn off UAC

1. Click **Start**, and then click **Control Panel**.
2. In **Control Panel**, click **User Accounts**.
3. In the **User Accounts** window, click **User Accounts**.
4. In the **User Accounts** tasks window, click **Turn User Account Control on or off**.
5. If UAC is currently configured in Admin Approval Mode, the **User Account Control** message appears. Click **Continue**.
6. Clear the **Use User Account Control (UAC) to help protect your computer** check box, and then click **OK**.
7. Click **Restart Now** to apply the change right away, or click **Restart Later**, and then close the **User Accounts**

tasks window.

Disabling Admin Approval Mode

Use the following procedure to disable Admin Approval Mode.

Note

To perform the following procedure, you must be logged on to a client computer as a local administrator.

Important

You cannot disable Admin Approval Mode on Windows Vista Starter, Windows Vista Home Basic, or Windows Vista Home Premium because secpol.msc is not included.

To disable Admin Approval Mode

1. Click **Start**, click **All Programs**, click **Accessories**, click **Run**, type **secpol.msc** in the **Open** box, and then click **OK**.
2. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**..
3. From the Local Security Settings console tree, double-click **Local Policies**, and then double-click **Security Options**.
4. Scroll down and double-click **User Account Control: Run all administrators in Admin Approval Mode**.
5. Select the **Disabled** option, and then click **OK**.
6. Close the **Local Security Settings** window.

Disabling User Account Control from prompting for credentials to install applications

Use the following procedure to disable UAC from prompting for credentials to install applications.

Note

To perform the following procedure, you must be logged on to a client computer as a local administrator.

Important

This procedure is not supported on Windows Vista Starter, Windows Vista Home Basic, or Windows Vista Home Premium.

To disable UAC from prompting for credentials to install applications

1. Click **Start**, click **All Programs**, click **Accessories**, click **Run**, type **secpol.msc** in the **Open** text box, and then click **OK**.
2. From the Local Security Settings console tree, click **Local Policies**, and then click **Security Options**.
3. Scroll down and double-click **User Account Control: Detect application installations and prompt for elevation**.
4. Select the **Disabled** option, and then click **OK**.
5. Close the **Local Security Settings** window.

Changing the elevation prompt behavior

Use the following procedures to change the elevation prompt behavior for UAC. You can configure the behavior of the elevation prompt separately for administrators and for standard users.

Note

To perform the following procedures, you must be logged on to a client computer as a local administrator.

Important

To complete the following procedures, you must be running Windows Vista Ultimate, Windows Vista Enterprise, or Windows Vista Business. You cannot complete the following procedures if you are running Windows Vista Starter, Windows Vista Home Basic, or Windows Vista Home Premium because secpol.msc is not included.

To change the elevation prompt behavior for administrators

1. Click **Start**, click **Accessories**, click **Run**, type **secpol.msc** in the **Open** box, and then click **OK**.
2. From the Local Security Settings console tree, click **Local Policies**, and then click **Security Options**.
3. Scroll down to and double-click **User Account Control: Behavior of the elevation prompt for administrators**.
4. From the drop-down menu, select one of the following settings:
   - **Elevate without prompting** (tasks that request elevation will automatically run as elevated without prompting the administrator)
   - **Prompt for credentials** (this setting requires user name and password input before an application or task will run as elevated)
   - **Prompt for consent** (default setting for administrators)
5. Click **OK**.

6. Close the **Local Security Settings** window.

To change the elevation prompt behavior for standard users

1. Click **Start**, click **Accessories**, click **Run**, type **secpol.msc** in the **Open** box, and then click **OK**.
2. From the Local Security Settings console tree, click **Local Policies**, and then **Security Options**.
3. Scroll down to and double-click **User Account Control: Behavior of the elevation prompt for standard users**.
4. From the drop-down menu, select one of the following settings:
   - **Automatically deny elevation requests** (standard users will not be able to run programs that require elevation, and they will not be prompted)
   - **Prompt for credentials** (this setting requires user name and password input before an application or task will run as elevated, and it is the default for standard users)
5. Click **OK**.
6. Close the **Local Security Settings** window.

Troubleshooting and support

Because UAC is a feature in Windows 7 Windows Vista, Windows Server 2008 R2, and Windows Server 2008, support is available directly from Microsoft and from user communities. For more information, see the Microsoft Support site.

Additional resources