



# Windows Vista™

## **Windows Vista Beta 2 User Account Control Step-by-Step Guide**

---

Microsoft Corporation

Published: December 2005

### **Abstract**

User Account Control (UAC) is a set of new infrastructure technologies in Microsoft® Windows Vista™ that helps organizations deploy a better-managed desktop and mitigate the impact of malware. This guide includes system requirements and step-by-step instructions on how to use UAC in a test lab environment.

**Microsoft**

This document supports a preliminary release of a software product that may be changed substantially prior to final commercial release, and is the confidential and proprietary information of Microsoft Corporation. It is disclosed pursuant to a non-disclosure agreement between the recipient and Microsoft. This document is provided for informational purposes only and Microsoft makes no warranties, either express or implied, in this document. Information in this document, including URL and other Internet Web site references, is subject to change without notice. The entire risk of the use or the results from the use of this document remains with the user. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2005 Microsoft Corporation. All rights reserved.

Microsoft, Windows, Windows Vista, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

References to any third-party products or their hardware identifiers are for illustrative purposes only. These product is not endorsed by Microsoft Corporation.

All other trademarks are property of their respective owners.

# Contents

---

Windows Vista Beta 2 User Account Control Step by Step Guide .....	5
What is User Account Control .....	5
Who should use this guide? .....	6
Why use this guide?.....	6
In this guide .....	6
Requirements for User Account Control.....	6
Setting up the test lab.....	7
Key scenarios for User Account Control.....	7
Scenario 1: Request an application to run elevated one time .....	7
Scenario 2: Mark an application to always run elevated .....	8
Scenario 3: Configure User Account Control .....	9
Disable Admin Approval Mode.....	9
Disable User Account Control from prompting for credentials to install applications ..	9
Change the elevation prompt behavior .....	10
Logging bugs and feedback .....	11
Additional resources .....	11
Technology Adoption Program support.....	11



# Windows Vista Beta 2 User Account Control Step by Step Guide

---

This Step-by-Step Guide provides the instructions necessary to use User Account Control (UAC) in a test lab environment.

## What is User Account Control

UAC is a new set of infrastructure technologies in Microsoft® Windows Vista™ that helps organizations deploy a better-managed desktop and mitigate the impact of malware. UAC requires all users to run applications and tasks with a standard user account, limiting administrator-level access to authorized processes. It also allows desktops to be locked down, which stops unauthorized applications from installing and stops standard users from making inadvertent changes to system settings.

In Windows Vista, there are two levels of users: standard users and administrators. Standard users run applications with a user account and are member of the Users group. Administrator users run applications with an administrator account and are members of the local Administrators group. When a user launches an application, their access token and its associated administrative privileges are applied to the application at run time. This means that an application launched by a member of the Administrators group runs with all rights and privileges allotted to a local administrator. Likewise, if a member of the Users group launches the same application, it runs with the rights and privileges allotted to a standard user.

In Windows Vista, most applications are supplied with either an "administrator" or "standard" token. If an application cannot be identified as an administrative application, Windows Vista will launch it as a standard application by default. Before an application identified as administrative can be launched, Windows Vista will prompt the user for consent to run the application as elevated. This feature is known as Admin Approval Mode. The consent prompt is displayed by default, even if the user is a member of the local Administrators group, because administrators run as standard users until an application or system component that requires administrative credentials requests permission to run. This process is called elevation.

The impact of malicious software can be reduced by notifying users when they are about to perform an action that could impact system settings, such as installing an application. When a user provides appropriate credentials, Windows Vista takes steps to protect the

administrative application from attacks by standard applications and processes. Because an administrator must approve application installations, unauthorized applications cannot be installed automatically. Additionally, standard users are prevented from making system-wide changes to operating system settings.

## Who should use this guide?

This guide is intended for the following audiences:

- IT planners and analysts who are evaluating the product.
- Early adopters.
- Security architects who are responsible for implementing trustworthy computing.

## Why use this guide?

The groups listed above should use this guide to test how their line-of-business (LOB) applications run in Windows Vista. Because UAC makes a clear distinction between administrator and standard user processes, some existing LOB applications may need to be either redesigned by the independent software vendor (ISV) or internal tools team, or marked to always run elevated.

## In this guide

- [Requirements for User Account Control](#)
- [Key scenarios for User Account Control](#)
- [Scenario 1: Requesting an application to run elevated one time](#)
- [Scenario 2: Marking an application to always run elevated](#)
- [Scenario 3: Configure User Account Control](#)
- [Logging bugs and feedback](#)
- [Additional Resources](#)

## Requirements for User Account Control

We recommend that you first use the steps provided in this guide in a test lab environment. Step-by-Step guides are not necessarily meant to be used to deploy Windows Vista features without accompanying documentation (as listed in the Additional Resources section), and 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 Microsoft Windows Server™ Code Name "Longhorn" (or Microsoft Windows Server 2003) a member server running Windows Server "Longhorn" (or Windows Server 2003), and a client computer running Windows Vista. The domain controller, member server, and the client computer should be on an isolated network and should be connected through a common hub or Layer 2 switch. Private addresses should be used throughout the test lab configuration.

## Key scenarios for User Account Control

This guide covers the following scenarios for UAC:

- [Scenario 1: Request an application to run elevated one time](#)
- [Scenario 2: Mark an application to always run elevated](#)
- [Scenario 3: Configure User Account Control](#)

### Note

The three scenarios included in this guide are intended to help administrators become familiar with the UAC feature of Windows Vista. They include the basic information and procedures 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 a member of the local Administrators group attempts 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 into a client computer as a member of the local administrators group. You cannot be logged in with the computer (or built-in) administrator account because Admin Approval Mode does not apply to this account.

 **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 Windows Security prompt is displayed.
2. From the Windows Security prompt, select **Permit** to start the application.

## Scenario 2: Mark an application to always run elevated

Scenario 2 is similar to the previous scenario in that you are giving approval to run an application or process as elevated with the administrator access token. However, in this scenario you are authorizing the application or process to always run elevated without prompting the user for consent. The following procedure steps you through that process.

 **Note**

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

 **To mark an application to always run elevated**

1. Right-click an application that is likely to have been assigned an administrative token, such as Microsoft Windows Disk Cleanup.
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 either the application is blocked from always running elevated, the application does not require administrative credentials to

run, or you are not logged into the computer as an administrator.

## Scenario 3: Configure User Account Control

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

### Disable Admin Approval Mode

Use the following procedure to disable Admin Approval Mode.

#### Note

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

#### To disable Admin Approval Mode

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: Run all users, including administrators, as standard users**.
4. From the **User Account Control: Run all users, including administrators, as standard users Properties** settings box, click **Disabled**.

### Disable 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 into a client computer as a local administrator.

▶ **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 **Security Options**.
3. Scroll down and double-click **User Account Control: Elevate on application installs**.
4. From the **User Account Control: Elevate on application installs Properties** settings box, click **Disabled**.

## Change the elevation prompt behavior

Use the following procedure to change the elevation prompt behavior for UAC.

 **Note**

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

▶ **To change the elevation prompt behavior**

1. Click **Start**, 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 **Security Options**.
3. Scroll down to and double-click **User Account Control: Behavior of the elevation prompt for administrators** or **User Account Control: Behavior of the elevation prompt for standard users**.
4. From the drop-down menu, select one of the following settings:
  - **No prompt**
  - **Prompt for credentials** (this setting requires user name and password input before an application or task will run as elevated)
  - **Prompt for consent** (this is the default setting for administrators only)

## Logging bugs and feedback

Since UAC is a new feature of Windows Vista, we are very interested in your feedback on your experiences with UAC, problems you encountered, and the usefulness of the documentation.

When you log bugs, use the instructions on the [Microsoft Connect Web site](http://go.microsoft.com/fwlink/?LinkId=49779) (<http://go.microsoft.com/fwlink/?LinkId=49779>). We are also interested in requests and general feedback about UAC.

General feedback and requests for UAC can be sent to [uacdoc@microsoft.com](mailto:uacdoc@microsoft.com).

## Additional resources

The following resources provide additional information about UAC:

- If you need product support, see the [Microsoft Connect Web site](http://go.microsoft.com/fwlink/?LinkId=49779) (<http://go.microsoft.com/fwlink/?LinkId=49779>).
- To access newsgroups for UAC, follow the instructions that are provided on the [Microsoft Connect Web site](http://go.microsoft.com/fwlink/?LinkId=50067) at <http://go.microsoft.com/fwlink/?LinkId=50067>.

Additional information for IT professionals is available on TechNet:

- [Getting Started with User Account Protection in Windows Vista Beta 1](http://go.microsoft.com/fwlink/?LinkID=56402) (<http://go.microsoft.com/fwlink/?LinkID=56402>)

Additional information for ISVs and developers is available on MSDN:

- [Developer Best Practices and Guidelines for Applications in a Least-Privileged Environment](http://go.microsoft.com/fwlink/?LinkID=56403) (<http://go.microsoft.com/fwlink/?LinkID=56403>)

## Technology Adoption Program support

If you are a beta tester and part of the special Technology Adoption Program (TAP) beta program, you can also contact your appointed Microsoft development team member for assistance.