



Windows Vista™

Step-by-Step Guide to Managing Multiple Local Group Policy

Microsoft Corporation

Published: August 2006

Author: Michael Stephens

Editor: Craig Liebendorfer

Abstract

This guide introduces IT administrators to the fundamental concepts needed to successfully configure Multiple Local Group Policy objects on stand-alone computers running Windows Vista™. This document includes a technical overview and several task-based scenarios that show you how to use this new feature. Each scenario builds on the previous scenario to help you understand how Windows applies each Local Group Policy object and how it resolves conflicts with policy settings. Each scenario closes with a review, explaining the intent and outcome of each scenario.

Microsoft

This document supports a preliminary release of a software product that may be changed substantially prior to final commercial release. 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 companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. 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.

© 2006 Microsoft Corporation. All rights reserved.

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

All other trademarks are property of their respective owners.

Contents

Step-by-Step Guide to Managing Multiple Local Group Policy Objects	5
Technology Review	5
Local Group Policy	6
Administrators and Non-Administrators Local Group Policy	6
User-Specific Group Policy	6
Processing order	7
Conflict resolution between policy settings	7
Domain member computers	7
Guide Requirements	8
Prerequisites	8
Check the current state	9
Create a custom management console	9
Multiple Local Group Policy Scenarios	11
Local Group Policy scenario	12
Check the results of the Local Group Policy object	13
Non-Administrators Local Group Policy scenario	13
Check the results of the Non-Administrators Local Group Policy object	14
Administrators Local Group Policy	15
Check the results of the Administrators Local Group Policy object	15
User-Specific Local Group Policy scenario	16
Check the results for the user-specific Local Group Policy object	17
Delete a Local Group Policy object	18
Check the results after deleting a Local Group Policy object	19
Summary	20
Appendix A: Local Group Policy Settings	20
Appendix B: Non-Administrators Local Group Policy Settings	21
Appendix C: User-Specific Local Group Policy Settings	23

Step-by-Step Guide to Managing Multiple Local Group Policy Objects

Securing computers and users' desktops is an important responsibility of the IT administrator. Today's computing environment provides users with hundreds, if not thousands, of configurable settings. Some of these settings are harmless while others could keep help desk staff busy. Domain administrators solve these tough problems using Group Policy. How do you solve this problem for stand-alone computers? Microsoft Windows Vista solves this problem by introducing Multiple Local Group Policy objects.

Multiple Local Group Policy objects (MLGPO) is a new feature included in Windows Vista that improves previous Local Group Policy technology found in Microsoft® Windows® XP. MLGPOs allow an administrator to apply different levels of Local Group Policy to local users on a stand-alone computer. This technology is ideal for shared computing environments where domain-based management is not available, such as shared library computers or public Internet kiosks

This guide includes a series of step-by-step scenarios to show how to set up Multiple Local Group Policy objects on a stand-alone computer running Windows Vista. These scenarios, when done in succession, will show you the power and flexibility of Multiple Local Group Policy objects, and will give you an understanding of MLGPOs and how to introduce them in your environment.

Technology Review

Local Group Policy is a subset of a broader technology known as Group Policy. Group Policy is domain based while Local Group Policy is specific to the local computer. Both technologies allow administrators to configure specific settings in the operating system and then force those settings to computers and users. Local Group Policy is not as robust as Group Policy. For example, Group Policy allows administrators to configure any number of policies that could affect some, all, or none of the users of a domain-joined computer. Group Policy could even apply policies to users that have specific group memberships. However, Local Group Policy could only apply one policy to the computer and all the local users of the computer, even the local administrator. This made managing the stand-alone computer difficult because the same policy applied to the administrator and the users.

Windows Vista introduces Multiple Local Group Policy objects, an improvement over the previous version of Local Group Policy that gives stand-alone computer administrators the ability to apply different Group Policy objects to stand-alone users. Windows Vista

provides this ability with three layers of Local Group Policy objects: Local Group Policy, Administrators and Non-Administrators Group Policy, and user specific Local Group Policy. These layers of Local Group Policy objects are processed in order, starting with Local Group Policy, continuing with Administrators and Non-Administrators Group Policy, and finishing with user-specific Local Group Policy.

Local Group Policy

The Local Group Policy (also known as Local Computer Policy) layer is the topmost layer in the list of Multiple Local Group Policy objects. Local Group Policy is the only Local Group Policy object that allows computer settings. Besides computer settings, you can select user settings. However, user settings contained in the Local Group Policy apply to all users of the computer, even the local administrator. Local Group Policy behaves the same as it did in Windows XP.

Administrators and Non-Administrators Local Group Policy

Each stand-alone computer running Windows Vista has a list of built-in groups and users. Windows Setup creates this list of users and groups during the installation or upgrade to Windows Vista. One of these groups is the administrators group. The administrators group is a built-in group created by Windows and by default has only one member, the administrator. Windows considers all members of the administrators group to be administrators of the computer. If the user is not a member of the local administrators group, then Windows considers the user to be a member of the local users group (non-administrators).

Administrators and Non-Administrators Local Group Policy objects act as a single layer and logically sort all local users into two groups when a user logs on to the computer. The user is either an administrator or a non-administrator. Users that are members of the administrators group receive policy settings assigned in the Administrators Local Group Policy object. All other users receive policy settings assigned in the Non-Administrators Local Group Policy objects. The Administrators and Non-Administrators Local Group Policy objects are new in Windows Vista.

User-Specific Group Policy

Administrators of stand-alone computers can create new local user accounts. When created, Windows stores these new accounts with the list of built-in groups and users on the local computer. Local administrators can use the last layer of the Local Group Policy object, Per-User Local Group Policy objects, to apply specific policy settings to a specific local user.

Processing order

The benefits of Multiple Local Group Policy objects come from the processing order of the three separate layers. The Local Group Policy object applies first. This Local Group Policy object may contain both computer and user settings. User settings contained in this policy apply to all users, including the local administrator. Next, Windows applies Administrators and Non-Administrators Local Group Policy objects. These two Local Group Policy objects represent a single layer in the processing order, and the user receives one or the other. Neither of these Local Group Policy objects contains computer settings. Windows finishes processing Local Group Policy objects by applying user-specific Local Group Policy. This last layer of Local Group Policy objects contains only user settings, and you apply it to one specific user on the local computer.

To summarize, Windows applies Local Group Policy objects first, then the Administrators or Non-Administrators Local Group Policy objects, and finally the user-specific Local Group Policy objects.

Conflict resolution between policy settings

Available user settings are the same between all Local Group Policy objects. It is conceivable a policy setting in one Local Group Policy object can contradict the same setting in another Local Group Policy object. Windows Vista resolves these conflict by using the "Last Writer Wins" method. This method resolves the conflict by overwriting any previous setting with the last read (most current) setting. The final setting is the one Windows uses.

For example, an administrator enables a setting in the Local Group Policy object. The administrator then disables the same setting in a user-specific Local Group Policy object. The user logging on to the computer is not an administrator. Windows reads the Local Group Policy object first, followed by the Non-Administrators Local Group Policy object, and then the user-specific Local Group Policy object. The state of the policy setting is enabled when Windows reads the Local Group Policy object. The policy setting is not configured in the Non-Administrators Local Group Policy object. This has no affect on the state of the setting, so it remains enabled. The policy setting is disabled in the user-specific Local Group Policy object. This changes the state of the setting to disabled. Windows reads the user-specific Local Group Policy object last; therefore, it has the highest precedence. The Local Computer Policy has lowered precedence.

Domain member computers

Stand-alone computers benefit the most from Multiple Local Group Policy objects, wherein managing each computer is local. Domain-based computers apply Local Group Policy first and then domain-based policy. Windows Vista continues to use the "Last

Writer Wins" method for conflict resolution. Therefore, policy settings originating from domain Group Policy overwrite any conflicting policy settings found in any Local Group Policy to include administrative, non-administrative, and user specific Local Group Policy. Domain administrators can disable processing Local Group Policy objects on clients running Windows Vista by enabling the "Turn off Local Group Policy objects processing" policy setting in a domain Group Policy object. You can find this setting under Computer Configuration\Administrative Templates\System\Group Policy.

Guide Requirements

This guide requires you to have one computer running Windows Vista Beta 2 or later. You can read the most current hardware requirements at the Windows Vista Web site (<http://go.microsoft.com/fwlink/?LinkID=67153>). Also, these scenarios require two user accounts: one administrative user account and one non-administrative user account. The administrative user account is the user account you created during the installation of Windows Vista. The prerequisites section shows you how to create a non-administrative user account.

Prerequisites

Create a non-administrative user account

1. Log on to a computer running Windows Vista with an administrative user account.
2. Open the **Start** menu. Right-click **Computer**, and then click **Manage**.
3. Click the arrow next to **Local Users and Groups**.
4. Right-click **Users**, and then click **New User**.
5. Type the name of the user you will use in scenarios included in this guide. For example, if you want to name the user "webuser1" then you would type **webuser1** in the **Username** box and in the **Full name** box.
6. Type a password you will remember in the **Password** and **Confirm Password** boxes. For example, if you choose to use "Password1" for the password, then you would type **Password1** in both the **Password** and **Confirm Password** boxes.

Important

Passwords are case sensitive. The password you type in the **Password** and **Confirm Password** boxes must match to add the user account.

7. Clear the **User must change password at next logon** check box.

8. Select the **Password never expires** and **User cannot change password** check boxes.
9. Click **Create**, and then click **Close**. Click **File**, and then click **Exit**.

Check the current state

Before you begin using these scenarios, you need to examine the current state of the user you just created. These scenarios change specific elements of the user environment. Understanding the before and after states provides a clearer understanding of each scenario and its impact. Before the scenarios, icons and shortcut menus are visible from the Desktop and Start menu. You will remove visible icons and shortcut menus as you progress through each scenario, confirming you implemented the policy correctly.

▶ To check the current state of the newly created user

1. Log on to the workstation with the user account you created in the "Create a non-administrative user account" procedure. Close any startup applications, if this is the first time you are logging in with this user on this computer. Note that icons appear on the desktop.
2. Open the **Start** menu and make note of the icons displayed.
3. Right-click the taskbar. Note the shortcuts that appear in the shortcuts menu.
4. Click **Start**, click **All Programs**, click **Accessories**, and then click **Run**. Notice how the Run dialog appears. Click **Cancel**.
5. Open the **Start** menu, right-click **Internet Explorer**, and then click **Internet Properties**. The Internet Control Panel appears. Make a note of all the tabs on this dialog box, specifically the **Connections** tab.
6. Log off of the computer.

Create a custom management console

You access Multiple Local Group Policy objects using Group Policy Object Editor. You must add Group Policy Object Editor to the Microsoft Management Console for each Local Group Policy object you want to manage. You should consider creating a custom management console for Multiple Local Group Policy objects (MLGPOs) if you are going to manage many MLGPOs.

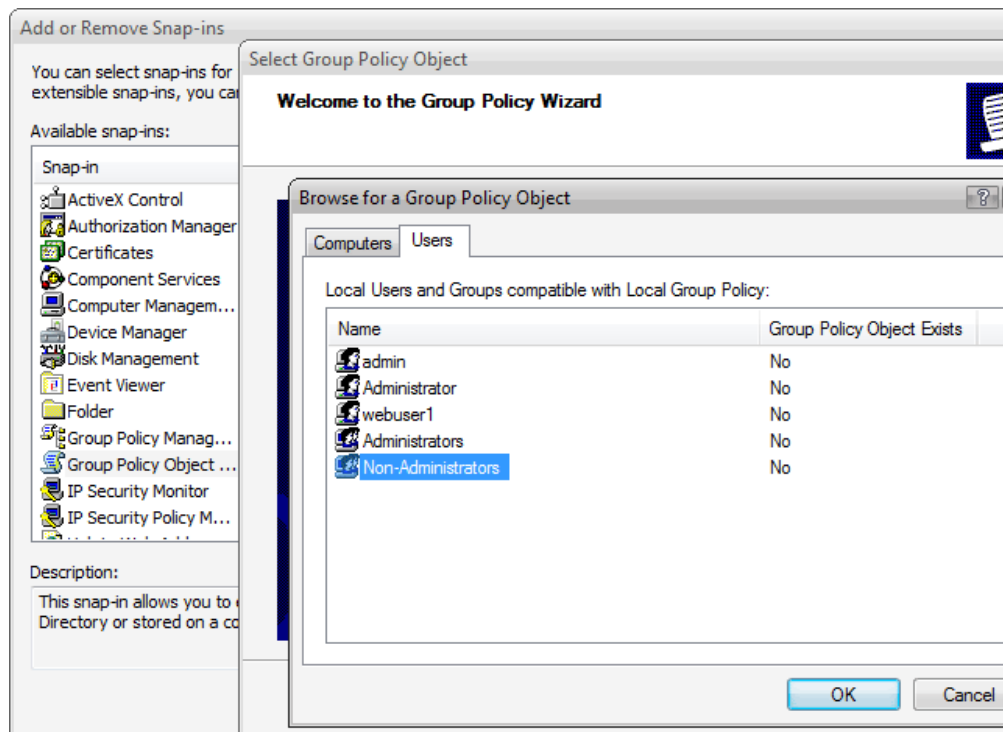
▶ To configure and save a custom management console

1. Log on to the workstation using the administrative account you created during the

installation of Windows Vista. Click **Start**, click **All Programs**, click **Accessories**, and then click **Run**. Type **mmc.exe** and click **OK**.

2. In the **Console1** window, click **File**, and then click **Add/Remove Snap-in**.
3. In the **Add/Remove Snap-in dialog box**, in the **Available snap-ins** list, click **Group Policy Object Editor**, and then click **Add**.
4. In the **Select Group Policy Object** dialog box, ensure **Local computer** appears under **Group Policy Object**. Click **Finish**.
5. Click **Group Policy Object Editor** under the **Available standalone snap-ins** list and then click **Add**.
6. In the **Select Group Policy Object** dialog box, click **Browse**. Click the **Users** tab. Click the **Non-Administrators** group. Click **OK**. Click **Finish**.

Figure 1 Browsing for the Non-Administrators Local Group Policy

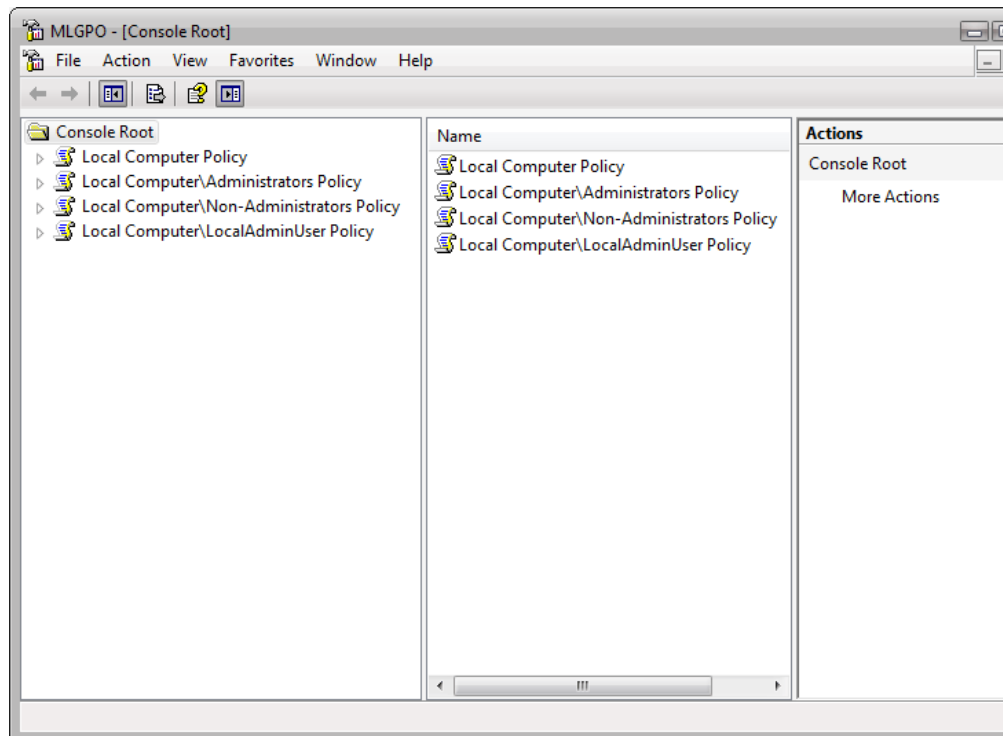


7. Click **Group Policy Object Editor** under the **Available standalone snap-ins** list and then click **Add**.
8. In the **Select Group Policy Object** dialog box, click **Browse**. Click the **Users** tab. Click the **Administrators** group. Click **OK**. Click **Finish**. Click **OK**.
9. Click **Group Policy Object Editor** under the **Available standalone snap-ins** list

and then click **Add**.

10. In the **Select Group Policy Object** dialog box, click **Browse**. Click the **Users** tab. Click the name of the administrative user you created during the installation of Windows Vista. For example, if you named your administrative user LocalAdminUser, then click **LocalAdminUser**. Click **OK**. Click **Finish**. Click **OK**.

Figure 2 View of the newly created MLGPO console



11. In the **Console1** window, click **File**, click **Save**, and then click **Desktop**. Type **MLGPO** in the filename text box and click **Save**.

 **Note**

You can start the custom management console by double-clicking the MLGPO icon located on your desktop.

Multiple Local Group Policy Scenarios

The following scenarios show you how to apply Group Policy settings in layers, using Multiple Local Group Policy objects. Each scenario ends with procedures to help you view the results of the policy settings. These procedures further show how each layer of

policy affects the logged-on user. You can then apply the principles learned in these scenarios to your own environment.

 **Note**

The policy settings in these scenarios change visual elements within the user environment, making it easier to notice changes for each Local Group Policy object. These policy settings are not the recommended policy settings for a kiosk scenario and are likely to change with each kiosk environment. Administrators should carefully consider all policy settings to decide which policy settings are proper for their environment.

Local Group Policy scenario

The Local Group Policy object contains both computer settings and user settings. You use Local Group Policy to apply policy settings specific to the computer and common policy settings that apply to all or most of the users of the computer.

In this scenario, you will configure policy settings using the list of policy settings in [Appendix A: Local Group Policy Settings](#) to complete this task. These policy settings affect the user interface of Internet Control Panel in Internet Explorer. Windows applies the Local Group Policy object to all users who log on to the computer.

Define Local Group Policy

1. Log on as the administrative user you created during the installation of Windows Vista. Double-click the MLGPO icon on your desktop that you created during the prerequisite portion of this document.
2. Click **Local Computer Policy**. Click the arrow next to **Administrative Templates** under the **User Configuration** node.
3. Click the arrow next to **Windows Components** and **Internet Explorer**. Click **Internet Control Panel**. Note the details pane shows all policies as **Not Configured**.
4. Use [Appendix A](#) to define each policy setting. When finished, close the MLGPO console by clicking **File** and then clicking **Exit**. If prompted to save the console, click **No**.

 **Note**

Local Computer Policy is also known as Local Group Policy in previous versions of Windows.

You have successfully defined policy settings in the Local Group Policy object. Now, check the results of the policy settings you performed in the Local Group Policy.

Check the results of the Local Group Policy object

In the "Local Group Policy scenario," you imposed policy settings that disabled specific tabs in the Internet Control Panel. The following procedure guides you through the user interface to view the results of the policy settings contained in the Local Group Policy object.

▶ Check the results

1. Log off of the computer. Log on to the computer using the user account created in the "Create a non-administrative user account" procedure.
2. Open the **Start** menu. Right-click **Internet Explorer**, and then click **Internet Properties**. The Internet Control Panel will appear with text that reads, "Access to this feature has been disabled by a restriction set by your system administrator."
3. Log off of the computer. Log on to the computer as the local administrative user. Perform step 2 again.

The "Local Group Policy scenario" shows you that Windows prevents access to the Internet Control Panel for the local administrative user and a normal user of the computer by using the Local Group Policy object.

Non-Administrators Local Group Policy scenario

The Non-Administrators Local Group Policy object contains user policy settings. Windows applies settings in this Local Group Policy object to users who are not members of the local administrators group.

In this scenario, you will configure policy settings in the Non-Administrators Group Policy object using the list of policy settings from [Appendix B: Non-Administrators Local Group Policy Settings](#). These policy settings will change the behavior of the Start menu and taskbar.

▶ Define Non-Administrators Local Group Policy

1. Log on to the workstation with the local administrative user account you created during the installation of Windows Vista..
2. Open the MLGPO console and click **Local Computer\Non-Administrators Policy**.
3. Click the arrow next to **Administrative Templates** under **User Configuration**. Click **Start Menu and Taskbar**.
4. Use the list of policy settings in [Appendix B](#) to define each policy setting. When finished, close the MLGPO console by clicking **File** and then clicking **Exit**. If

prompted to save the console, click **No**.

5. Log off of the computer.

You have successfully configured policy settings for the Non-Administrators Local Group Policy object. Check the results of adding the Non-Administrators Local Group Policy object and see how it works with the Local Group Policy object.

Check the results of the Non-Administrators Local Group Policy object

In the "Non-Administrators Local Group Policy scenario," you enabled user settings in the Non-Administrators Local Group Policy object. These procedures help you review the effects the Non-Administrators Local Group Policy object have on a local user and the local administrator. Icons appeared on the Desktop and Start menu before implementing the Non-Administrators Local Group Policy. After creating the policy, icons do not appear on the Desktop and Start menu. Also, shortcut menus are not available. This confirms you successfully created the Non-Administrators Local Group Policy.

Check the results

1. Log on to the workstation with the previously created user account. Icons do not appear on the desktop.
2. Open the **Start** menu. Icons are not displayed on the **Start** menu.
3. Right-click the taskbar. Notice that the shortcut menu does not appear.
4. Click **Start**, click **All Programs**, click **Accessories**, and then click **Run**. A warning dialog appears stating the system administrator has disabled the Run menu.
5. Log off of the computer. Log on as the local administrator you created during the installation of Windows Vista.
6. Repeat steps 3–5. Notice the different behavior in the **Start** menu and taskbar between a local user and the local administrator
7. Open the **Start** menu. Right-click **Internet Explorer**, and then click **Internet Properties**. The Internet Control Panel appears with text that reads, "Access to this feature has been disabled by a restriction set by your system administrator."

In the "Non-Administrators Local Group Policy scenario," you added policy settings to the Non-Administrators Local Group Policy that changed the behavior of the Start menu and taskbar. Non-administrative users did not have icons on their desktop or in their Start menu. Also, you removed non-administrative users' ability to use shortcut menus on the taskbar and the Run command.

Administrative users have icons on their desktop and Start menu. Taskbar shortcut menus and the Run command work properly. However, Windows still restricts administrative users from access to the Internet Control Panel. This restriction persists because you enabled it in the Local Group Policy and it applies to all local users. Non-administrative users are still affected by this policy; however, they are further restricted from accessing the Internet Control Panel because the icon is not present.

Administrators Local Group Policy

The Administrators Local Group Policy object contains user policy settings. Windows applies this Local Group Policy object to users who are members of the local administrators group. Use the Administrators Local Group Policy to set policy settings only for local administrators. In this scenario, you will set a single policy setting, which will add a command to the Start menu for administrators.

▶ Define Administrators Local Group Policy

1. Open the MLGPO console, and then click **Local Computer\Administrators Policy**.
2. Click the arrow next to the **Administrative Templates** under **User Configuration**.
3. Click **Start Menu and Taskbar**. The details pane shows all policies as **Not configured**.
4. In the details pane, double-click the **Add the Run command to the Start Menu** policy setting.
5. In the **Add the Run command to the Start Menu** dialog box, click **Enabled**. Click **OK** to finish.

You have successfully configured the Administrators Local Group Policy object. In this scenario, you added a single policy setting for all Administrators. Check the results of adding the Administrators Local Group Policy object and note how it works with the existing Local Group Policy.

Check the results of the Administrators Local Group Policy object

This policy setting adds the Run command to the Start menu. Use the following procedures to discover the effects this new Local Group Policy object has on the local administrator and user.

▶ Check the results

1. Log on to the computer as the local administrative user you created during the

installation of Windows Vista.

2. Open the **Start** menu. The **Run** command is located on the lower right of the **Start** menu.
3. Open the **Start** menu. Right-click **Internet Explorer**, and then click **Internet Properties**. The **Internet Control Panel** appears with text that reads, "Access to this feature has been disabled by a restriction set by your system administrator."
4. Log off of the computer. Log on as the non-administrative user.
5. Repeat steps 1 and 2. Non-administrative users do not have the **Run** command on the **Start** menu.

In the "Administrators Local Group Policy scenario," you added the policy setting to add the Run command from the Start menu to the Administrators Local Group Policy object. Then, as an administrator, you opened the Start menu to reveal the Run command. This scenario shows how you can set policy settings that apply only to local administrators. However, even as a local administrative user, you cannot access the Internet Control Panel because of the Local Group Policy object. Windows restricts non-administrative users' ability to invoke taskbar context menus, the Run command, and icons on the desktop or Start menu. If the icon were present, the non-administrative user would still not have access to the Internet Control Panel.

To review, in the first scenario, you disabled access to the Internet Control Panel in the Local Group Policy object. The results so far show the Local Group Policy is affecting administrative and non-administrative local users. Next, you enabled policy settings that restrict icons from the Desktop and the Start menu in the Non-Administrators Local Group Policy object. You viewed the results of these policy settings when the non-administrative user no longer had icons on their desktop or on the Start menu. However, none of these settings affected the administrative user, showing that the Non-Administrators Local Group Policy object is applying to users as its name suggests. In the last scenario, you used the Administrators Local Group Policy object to add the Run command to the Start menu. The results show Windows is applying this policy to administrative users only.

User-Specific Local Group Policy scenario

User-specific Local Group Policy objects contain user policy settings and apply to a specific local user. In this scenario, you will use the policy settings listed in [Appendix C: User-Specific Local Group Policy Settings](#) and create a user-specific Local Group Policy object for the local administrative user account you created during the installation of Windows Vista.

 **Note**

You should follow "Local Group Policy scenario" before following the current scenario. The policy settings in this scenario conflict with policy settings enabled in "Local Group Policy scenario." This scenario adds the Advanced, Content, General, Privacy, Programs, and Security tabs to the Internet Control Panel that you removed previously in "Local Group Policy scenario."

 **Define a user-specific Local Group Policy**

1. Log on to the computer with the local administrative account you created during the installation of Windows Vista.
2. Open the MLGPO console, and then click the node containing the name of the local administrative user account you created during the installation of Windows Vista. For example, if you named the user "LocalAdminUser," then you would click **Local Computer\LocalAdminUser**.
3. Click the arrow next to **Administrative Templates** under **User Configuration**. Click the arrow next to **Windows Components** and **Internet Explorer**. Click **Internet Control Panel**.
4. Refer to [Appendix C](#) to define each policy setting. When finished, close the MLGPO console by clicking **File** and then clicking **Exit**. If prompted to save the console, click **No**.

You have successfully defined a user-specific Local Group Policy object.

Check the results for the user-specific Local Group Policy object

The "User-Specific Local Group Policy scenario" enabled the Advanced, Content, General, Privacy, Programs, and Security tabs to the Internet Control Panel. These policy settings were previously disabled in the "Local Group Policy" scenario.

 **Check the results**

1. Log on to the computer with the local administrative user account you created during the installation of Windows Vista.
2. Open the **Start** menu. Right click **Internet Explorer**. Click **Internet Properties**. Windows displays the **Internet Control Panel** and all the tabs except the **Connections** tab.
3. Open the **Start** menu. The **Run** command is located on the lower right of the **Start** menu.

The Local Group Policy scenario prevented a local administrative user from opening the Internet Control Panel. Windows applies the user-specific Local Group Policy for the

Administrator last and therefore has precedence over conflicting settings. This behavior allows only the specific administrative user access to the Internet Control Panel. The absence of the Connections tab within the Internet Control Panel shows Windows is still applying the Local Group Policy.

These scenarios show one of many ways you can configure Multiple Local Group Policy objects. You can use Local Group Policy to set global limits and then use the Administrators, Non-Administrators, and user-specific Local Group Policy objects to remove the limits. Alternatively, you can use each Local Group Policy to restrict the respective group or user it applies to.

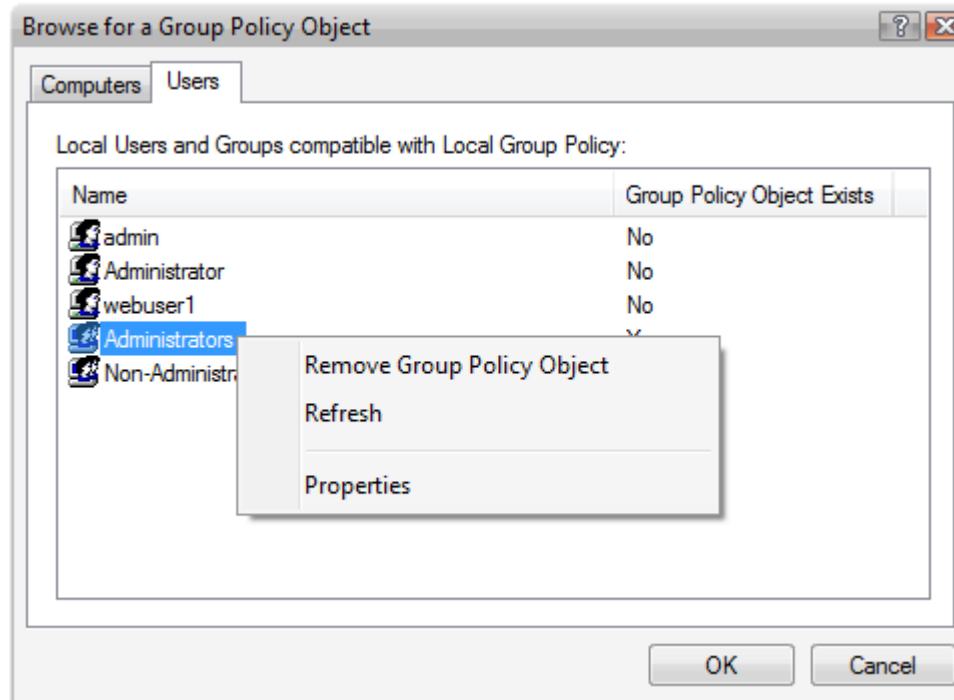
Delete a Local Group Policy object

Occasionally you may need to remove the entire Local Group Policy object rather than change multiple policy settings. Use the following procedure to delete the Administrators, Non-Administrators, and user-specific Local Group Policy objects. You cannot delete the Local Group Policy object. You must set each policy setting to Not Configured to return the Local Group Policy object to the default settings.

▶ To delete a Local Group Policy object

1. Log on to the computer with the local administrative user account you created during the installation of Windows Vista.
2. Double-click the MLGPO icon on the desktop. Click **File**, and then click **Add/Remove snap-in**.
3. Click **Group Policy Object Editor** under the **Available standalone snap-ins** list, and then click **Add**.
4. In the **Select Group Policy Object** dialog box, click **Browse**. Click the **Users** tab. Right-click the **Administrators** group. Click **Remove Group Policy Object**.

Figure 3 Removing a Local Group Policy



5. Click **Yes** to confirm the deletion of the Local Policy object. The text located in the **Group Policy Object Exists** column next to **Administrators** will display **No**.
6. Click **Cancel** three times to return to the MLGPO console.
7. Click **File**, and then click **Exit** to close the MLGPO console. Click **No**, if prompted to save the console.
8. Log off of the computer.

Check the results after deleting a Local Group Policy object

When you delete a Local Group Policy object, you change all the defined policy settings back to Not Configured. This removes any of the policy settings that you previously applied to the user.

► Check the results

1. Log on to the computer as the local administrative user you created during the installation of Windows Vista.
2. Open the **Start** menu. The **Start** menu no longer shows the **Run** command that you defined in the "*Administrators Local Group Policy* scenario."

Summary

Windows Vista introduces greater flexibility in managing Local Group Policy objects, providing the means to manage Multiple Local Group Policy objects on a single computer. This increased flexibility eases managing environments that involve shared computing on a single computer—such as libraries or computer labs—allowing each computer to keep its own policy settings. In Windows Vista, this flexibility is manifested through computer, group, and user-specific Local Group Policy objects, making Multiple Local Group Policies the ideal Group Policy Management solution for stand-alone computers.

Appendix A: Local Group Policy Settings

You should not change any policy settings that do not appear in this appendix. Changing additional policy settings may alter the results of the scenarios described in this guide.

Location	Policy	State
Internet Explorer\Internet Control Panel	Disable the Advanced page	Enabled
Internet Explorer\Internet Control Panel	Disable the Connections page	Enabled
Internet Explorer\Internet Control Panel	Disable the Content page	Enabled
Internet Explorer\Internet Control Panel	Disable the General page	Enabled
Internet Explorer\Internet Control Panel	Disable the Privacy page	Enabled
Internet Explorer\Internet Control Panel	Disable the Programs page	Enabled
Internet Explorer\Internet Control Panel	Disable the Security page	Enabled

Appendix B: Non-Administrators Local Group Policy Settings

You should not change any policy settings that do not appear in this appendix. Changing additional policy settings may alter the results of the scenarios described in this guide.

Location	Policy	State
Start Menu and Taskbar	Remove user's folders from the Start Menu	Enabled
Start Menu and Taskbar	Remove links and access to Windows Update	Enabled
Start Menu and Taskbar	Remove common program groups from Start Menu	Enabled
Start Menu and Taskbar	Remove Documents icon from Start Menu	Enabled
Start Menu and Taskbar	Remove programs on Settings menu	Enabled
Start Menu and Taskbar	Remove Network Connections from Start Menu	Enabled
Start Menu and Taskbar	Remove Favorites menu from Start Menu	Enabled
Start Menu and Taskbar	Remove Search link from Start Menu	Enabled
Start Menu and Taskbar	Remove Help menu from Start Menu	Enabled
Start Menu and Taskbar	Remove Run menu from Start Menu	Enabled
Start Menu and Taskbar	Remove Pictures icon from Start Menu	Enabled
Start Menu and Taskbar	Remove Music icon from Start Menu	Enabled
Start Menu and Taskbar	Remove Network icon from Start Menu	Enabled

Location	Policy	State
Start Menu and Taskbar	Add Logoff to the Start Menu	Enabled
Start Menu and Taskbar	Remove and prevent access to the Shut Down command	Enabled
Start Menu and Taskbar	Remove Drag-and-drop menus on the Start Menu	Enabled
Start Menu and Taskbar	Prevent changes to Taskbar and Start Menu Settings	Enabled
Start Menu and Taskbar	Remove access to the context menus for the taskbar	Enabled
Start Menu and Taskbar	Do not keep history of recently opened documents	Enabled
Start Menu and Taskbar	Clear history of recently opened documents on exit	Enabled
Start Menu and Taskbar	Turn off personalized menus	Enabled
Start Menu and Taskbar	Turn off user tracking	Enabled
Start Menu and Taskbar	Prevent grouping of taskbar items	Enabled
Start Menu and Taskbar	Remove Balloon Tips on Start Menu items	Enabled
Start Menu and Taskbar	Remove pinned programs list from the Start Menu	Enabled
Start Menu and Taskbar	Remove the "Undock PC" button from the Start Menu	Enabled
Start Menu and Taskbar	Do not display any custom toolbars in the taskbar	Enabled
Start Menu and Taskbar	Prevent grouping of taskbar items	Enabled
Desktop	Remove My Documents icon on the desktop	Enabled

Location	Policy	State
Desktop	Remove My Computer icon on the desktop	Enabled
Desktop	Remove Recycle Bin icon from desktop	Enabled
Desktop	Remove Properties from the My Documents context menu	Enabled
Desktop	Remove Properties from the My Computer context menu	Enabled
Desktop	Remove Properties from the Recycle Bin context menu	Enabled
Desktop	Hide My Network Places icon on desktop	Enabled
Desktop	Prohibit adjusting desktop toolbars	Enabled
Desktop	Don't save settings at exit	Enabled

Appendix C: User-Specific Local Group Policy Settings

You should not change any policy settings that do not appear in this appendix. Changing additional policy settings may alter the results of the scenarios described in this guide.

Location	Policy	State
Internet Explorer\Internet Control Panel	Disable the Connections page	Not Configured
Internet Explorer\Internet Control Panel	Disable the Advance page	Disabled
Internet Explorer\Internet Control Panel	Disable the Content page	Disabled
Internet Explorer\Internet Control Panel	Disable the General page	Disabled

Location	Policy	State
Internet Explorer\Internet Control Panel	Disable the Privacy page	Disabled
Internet Explorer\Internet Control Panel	Disable the Programs page	Disabled
Internet Explorer\Internet Control Panel	Disable the Security page	Disabled