Microsoft®

Windows® 7

William R. Stanek
Author and Series Editor

Administrator's Pocket Consultant

Microsoft®

Windows® 7

Administrator's Pocket Consultant

William R. Stanek

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Library of Congress Control Number: 2009932696

Printed and bound in the United States of America.

1 2 3 4 5 6 7 8 9   QWE   4 3 2 1 0 9

Distributed in Canada by H.B. Fenn and Company Ltd.

A CIP catalogue record for this book is available from the British Library.

Microsoft Press books are available through booksellers and distributors worldwide. For further information about international editions, contact your local Microsoft Corporation office or contact Microsoft Press International directly at fax (425) 936-7329. Visit our Web site at www.microsoft.com/mspress. Send comments to mspinput@microsoft.com.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted 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.

This book expresses the author’s views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. Neither the authors, Microsoft Corporation, nor its resellers, or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

Acquisitions Editor: Juliana Aldous
Developmental Editor: Karen Szall
Project Editor: Carol Vu
Editorial Production: Publishing.com
Technical Reviewer: Jim Johnson; Technical Review services provided by Content Master, a member of CM Group, Ltd.
Cover: Tom Draper Design

Body Part No. X15-74130

Contents

Chapter 16 Managing Mobile Networking and Remote Access 575

Introduction

Writing *Windows 7 Administrator's Pocket Consultant* was a lot of fun—and a lot of work. As I set out to write this book, my initial goals were to determine how Windows 7 was different from Windows Vista and Windows XP and what new administration options were available. As with any new operating system—but especially with Windows 7—I had to do a great deal of research and a lot of digging into the operating system internals to determine exactly how things work.

When you start working with Windows 7, you'll see at once that the operating system is different from earlier releases of Windows. What won't be apparent, however, is just how different Windows 7 is from its predecessors—and that's because many of the most significant changes to the operating system are below the surface. These changes affect the underlying architecture, as well as the user interfaces, and they were some of the hardest for me to research and write about.

Because Administrator's Pocket Consultants are meant to be portable and readable—the kind of book you use to solve problems and get the job done wherever you might be—I had to carefully review my research to make sure I focused on the core aspects of Windows 7 administration. The result is the book you hold in your hands, which I hope you'll agree is one of the best practical, portable guides to Windows 7. Toward that end, the book covers everything you need to perform the core administrative tasks for computers running Windows 7.

Because my focus is on giving you maximum value in a pocket-size guide, you don't have to wade through hundreds of pages of extraneous information to find what you're looking for. Instead, you'll find exactly what you need to address a specific issue or perform a particular task. In short, the book is designed to be the one resource you turn to whenever you have questions regarding Windows 7 administration. It zeroes in on daily administration procedures, frequently used tasks, documented examples, and options that are representative while not necessarily inclusive.

One of the goals for this book is to keep its content concise so that it remains compact and easy to navigate while at the same time packing it with as much information as possible to make it a valuable resource. Instead of a hefty 1,000-page tome or a lightweight, 100-page quick reference, you get a valuable resource guide that can help you quickly and easily perform common tasks, solve problems, and implement everyday solutions for systems and users.

Who Is This Book For?

Windows 7 Administrator's Pocket Consultant covers all editions of Windows 7. The book is designed for:

- Current Windows system administrators.
- Accomplished users who have some administrator responsibilities.
- Administrators upgrading to Windows 7 from earlier releases of Windows.
- Administrators transferring from other platforms.

To pack in as much information as possible, I had to assume that you have basic networking skills and a basic understanding of Windows operating systems. As a result, I don't devote entire chapters to understanding Windows basics, Windows architecture, or Windows networks. I do, however, cover desktop customization, mobile networking, TCP/IP configuration, user profiles, and system optimization. The book also goes into depth on troubleshooting, and I've tried to ensure that each chapter, where appropriate, has troubleshooting guidelines and discussions to accompany the main text. From the start, troubleshooting advice is integrated into the book—instead of being captured in a single, catchall troubleshooting chapter inserted as an afterthought. I hope that after you read these chapters and dig into the details, you'll be able to improve the overall experience of your users and reduce downtime.

How Is This Book Organized?

Windows 7 Administrator's Pocket Consultant is designed to be used in daily administration, and as such, the book is organized by job-related tasks rather than by Windows 7 features. The books in the Administrator's Pocket Consultant series are down-and-dirty, in-the-trenches books.

Speed and ease of reference are essential elements of this hands-on guide. The book has an expanded table of contents and an extensive index for finding answers to problems quickly. Many other quick reference features have been added as well. These features include step-by-step instructions, lists, tables with fast facts, and extensive cross-references.

Conventions Used in This Book

I've used a variety of elements to help keep the text clear and easy to follow. You'll find code listings in monospace type, except when I tell you to actually type a command. In that case, the command appears in **bold** type. When I introduce and define a new term, I put it in *italics*.

Other conventions include the following:

Note To provide additional details about a particular point that needs emphasis

Tip To offer helpful hints or additional information

Caution To warn you when there are potential problems you should look out for

Real World To provide real-world advice when discussing advanced topics

I truly hope you find that *Windows 7 Administrator's Pocket Consultant* provides everything you need to perform the essential administrative tasks on Windows 7 systems as quickly and efficiently as possible. You are welcome to send your thoughts to me at williamstanek@aol.com. Thank you.

Find Additional Content Online

As new or updated material becomes available that complements this book, it will be posted online on the Microsoft Press Online Windows Server and Client Web site. The type of material you might find includes updates to book content, articles, links to companion content, errata, sample chapters, and more. This Web site is available at *http://microsoftpresssrv.libredigital.com/serverclient/* and is updated periodically.

You'll also find discussion about the book at *www.williamstanek.com*. Follow me on Twitter at WilliamStanek.

Support

Every effort has been made to ensure the accuracy of this book. Microsoft Press provides corrections for books through the World Wide Web at the following address:

http://www.microsoft.com/mspress/support

If you have comments, questions, or ideas about this book, please send them to Microsoft Press using either of the following methods:

Postal mail:
Microsoft Press
Attn: Editor, *Windows 7 Administrator's Pocket Consultant*
One Microsoft Way
Redmond, WA 98052-6399

E-mail:
mspinput@microsoft.com

Please note that product support isn't offered through these addresses. For support information, visit Microsoft's Web site at *http://support.microsoft.com/.*

CHAPTER 5

Managing User Access and Security

Computers running Windows 7 can be configured to be members of a homegroup, a workgroup, or a domain. When a workstation is configured as a member of a homegroup or a workgroup, user access and security are configured on the workstation itself. When a workstation is configured as a member of a domain, user access and security are configured at two levels: the local system level and the domain level. User access can be configured at the local system level for a specific machine and at the domain level for multiple systems or resources throughout the current Active Directory forest. In this chapter, you'll learn how to manage local system access and local accounts. For further discussion of configuring domain access and permissions, see *Windows Server 2008 Administrator's Pocket Consultant,* Second Edition (Microsoft Press, 2010). Keep in mind that every task examined in this chapter and throughout this book can be performed through a local logon or a remote desktop connection.

Understanding User and Group Accounts

Windows 7 provides user accounts and group accounts (of which users can be members). User accounts are designed for individuals. Group accounts, usually referred to as *groups,* are designed to simplify the administration of multiple users. You can log on with a user account, but you can't log on with a group account.

Two general types of user accounts are defined in Windows 7:

- **Local user accounts** User accounts defined on a local computer are called *local user accounts.* These accounts have access to the local computer only. You add or remove local user accounts with Control Panel's User Accounts options or with the Local Users And Groups utility. Local Users And Groups is accessible through Computer Management, a Microsoft Management Console (MMC) snap-in.
- **Domain user accounts** User accounts defined in Active Directory are called *domain user accounts*. Through single sign-on, these accounts can access resources throughout a forest. When a computer is a member of an Active Directory domain, you can use it to create domain user accounts by using Active Directory Users And Computers. This MMC tool is available on the Administrative Tools menu when you install the Remote Server Administrator Tools on your Windows 7 computer.

Both local user accounts and domain user accounts can be configured as standard user accounts or administrator accounts. A standard user account on a local computer has limited privileges, and an administrator account on a local computer has extended privileges.

Local User Account Essentials

All user accounts are identified with a logon name. In Windows 7, this logon name has two parts:

- **User name** The display text for the account
- **User computer or domain** The computer or domain in which the user account exists

For the user Williams, whose account is created for the computer ENGPC85, the full logon name for Windows 7 is ENGPC85\Williams. With a local computer account, Williams can log on to his local workstation and access local resources but is not able to access domain resources.

When working with domains, the full logon name can be expressed in two different ways:

- The user account name and the full domain name separated by the At sign (@). For example, the full logon name for the user name Williams in the domain technology.microsoft.com would be *Williams@technology.microsoft.com*.
- The user account name and the domain separated by the backslash symbol (\). For example, the full logon name for Williams in the technology domain would be technology\Williams.

Although Windows 7 displays user names when describing account privileges and permissions, the key identifiers for accounts are security identifiers (SIDs). SIDs are unique identifiers generated when security principals are created. Each SID combines a computer or domain security ID prefix with a unique relative ID for the user. Windows 7 uses these identifiers to track accounts and user names independently. SIDs serve many purposes, but the two most important are to enable you to easily change user names and to delete accounts without worrying that someone might gain access to resources simply by re-creating an account.

When you change a user name, you tell Windows 7 to map a particular SID to a new name. When you delete an account, you tell Windows 7 that a particular SID is no longer valid. Even if you create an account with the same user name later, the new account won't have the same privileges and permissions as the previous one because the new account will have a new SID.

User accounts can also have passwords and certificates associated with them. Passwords are authentication strings for an account. Certificates combine a public and private key to identify a user. You log on with a password interactively, whereas you log on with a certificate by using its private key, which is stored on a smart card and read with a smart card reader.

When you install Windows 7, the operating system installs default user accounts. You'll find several built-in accounts, which have purposes similar to those of accounts created in Windows domains. The key accounts are the following:

- **Administrator** Administrator is a predefined account that provides complete access to files, directories, services, and other facilities. You can't delete or disable this account. In Active Directory, the Administrator account has domainwide access and privileges. On a local workstation, the Administrator account has access only to the local system.
- **Guest** Guest is designed for users who need one-time or occasional access. Although guests have only limited system privileges, you should be very careful about using this account because it opens the system to potential security problems. The risk is so great that the account is initially disabled when you install Windows 7.

By default, these accounts are members of various groups. Before you modify any of the built-in accounts, you should note the property settings and group memberships for the account. Group membership grants or limits the account's access to specific system resources. For example, Administrator is a member of the Administrators group and Guest is a member of the Guests group. Being a member of a group makes it possible for the account to use the privileges and rights of the group.

In addition to the built-in accounts, Windows 7 has several pseudo-accounts that are used to perform specific types of system actions. The pseudo-accounts are available only on the local system. You can't change the settings for these accounts with the user administration tools, and users can't log on to a computer with these accounts. The pseudo-accounts available include the following:

- **LocalSystem** LocalSystem is used for running system processes and handling system-level tasks. This account grants the logon right Log On As

A Service. Most services run under the LocalSystem account. In some cases, these services have privileges to interact with the desktop. Services that need fewer privileges or logon rights run under the LocalService or NetworkService account. Services that run as LocalSystem include Background Intelligent Transfer Service, Computer Browser, Group Policy Client, Netlogon, Network Connections, Print Spooler, and User Profile Service.

- **LocalService** LocalService is used for running services that need fewer privileges and logon rights on a local system. By default, services that run under this account are granted the right Log On As A Service and the privileges Adjust Memory Quotas For A Process, Change The System Time, Change The Time Zone, Generate Security Audits, and Replace A Process Level Token. Services that run as LocalService include Application Layer Gateway Service, Remote Registry, Smart Card, SSDP Discovery Service, TCP/IP NetBIOS Helper, and WebClient.
- **NetworkService** NetworkService is used for running services that need fewer privileges and logon rights on a local system but must also access network resources. Like services that run under LocalService, services that run by default under the NetworkService account are granted the right Log On As A Service and the privileges Adjust Memory Quotas For A Process, Generate Security Audits, and Replace A Process Level Token. Services that run under NetworkService include BranchCache, Distributed Transaction Coordinator, DNS Client, Remote Desktop Services, and Remote Procedure Call (RPC). NetworkService can also authenticate to remote systems as the computer account.

Group Account Essentials

Windows 7 also provides groups, which you use to grant permissions to similar types of users and to simplify account administration. If a user is a member of a group that has access to a resource, that user has access to the same resource. You can give a user access to various work-related resources just by making the user a member of the correct group. Although you can log on to a computer with a user account, you can't log on to a computer with a group account. Because different Active Directory domains or local computers might have groups with the same name, groups are often referred to by *Domain**GroupName* or *Computer**GroupName* (for example, Technology\GMarketing for the GMarketing group in a domain or on a computer named Technology).

Windows 7 uses the following three types of groups:

- **Local groups** Defined on a local computer and used on the local computer only. You create local groups with Local Users And Groups.
- **Security groups** Can have security descriptors associated with them. You use a Windows server to define security groups in domains, using Active Directory Users And Computers.

- **Distribution groups** Used as e-mail distribution lists. They can't have security descriptors associated with them. You define distribution groups in domains using Active Directory Users And Computers.

As with user accounts, group accounts are tracked using unique SIDs. This means that you can't delete a group account and re-create it and then expect that all the permissions and privileges remain the same. The new group will have a new SID, and all the permissions and privileges of the old group will be lost.

When you assign user access levels, you have the opportunity to make the user a member of the following built-in or predefined groups:

- **Administrators** Members of this group are local administrators and have complete access to the workstation. They can create accounts, modify group membership, install printers, manage shared resources, and more. Because this account has complete access, you should be very careful about which users you add to this group.
- **Backup Operators** Members of this group can back up and restore files and directories on the workstation. They can log on to the local computer, back up or restore files, and shut down the computer. Because of how this account is set up, its members can back up files regardless of whether the members have read/write access to the files. However, they can't change access permissions on the files or perform other administrative tasks.

  Backup Operators have privileges to perform very specific administrative tasks, such as backing up file systems. By default, no other group or user accounts are members of the operator groups. This is to ensure that you grant explicit access to the operator groups.
- **Cryptographic Operators** Members can manage the configuration of encryption, IP Security (IPSec), digital IDs, and certificates.
- **Event Log Readers** Members can view the event logs on the local computer.
- **Guests** Guests are users with very limited privileges. Members can access the system and its resources remotely, but they can't perform most other tasks.
- **Network Configuration Operators** Members can manage network settings on the workstation. They can also configure TCP/IP settings and perform other general network configuration tasks.
- **Performance Log Users** Members can view and manage performance counters. They can also manage performance logging.
- **Performance Monitor Users** Members can view performance counters and performance logs.
- **Power Users** In earlier versions of Windows, this group is used to grant additional privileges, such as the capability to modify computer settings and install programs. In Windows 7, this group is maintained only for compatibility with legacy applications.

- **Remote Desktop Users** Members can log on to the workstation remotely using Remote Desktop Services. Once members are logged on, additional groups of which they are members determine their permissions on the workstation. A user who is a member of the Administrators group is granted this privilege automatically. (However, remote logons must be enabled before an administrator can remotely log on to a workstation.)
- **Replicator** Members can manage the replication of files for the local machine. File replication is primarily used with Active Directory domains and Windows servers.
- **Users** Users are people who do most of their work on a single Windows 7 workstation. Members of the Users group have more restrictions than privileges. They can log on to a Windows 7 workstation locally, keep a local profile, lock the workstation, and shut down the workstation.

In most cases, you configure user access by using the Users or Administrators group. You can configure user and administrator access levels by setting the account type to Standard User or Administrator, respectively. While these basic tasks can be performed using Control Panel's User Accounts page, you make a user a member of a group by using Local Users And Groups under Computer Management.

Domain vs. Local Logon

When computers are members of a domain, you typically use domain accounts to log on to computers and the domain. All administrators in a domain have access to resources on the local workstations that are members of the domain. Users, on the other hand, can access resources only on the local workstations they are permitted to log on to. In a domain, any user with a valid domain account can by default log on to any computer that is a member of the domain. Once logged on to a computer, the user has access to any resource that his or her account or the groups to which the user's account belongs are granted access. This includes resources on the local machine as well as resources in the domain.

You can restrict logons to specific domain workstations on a per-user basis by using Active Directory Users And Computers. In Active Directory Users And Computers, right-click the user account and then click Properties. On the Account tab of the user's Properties dialog box, click Log On To, and then use the options in the Logon Workstations dialog box to designate the workstations to which the user is permitted to log on.

When you work with Windows 7, however, you aren't always logging on to a domain. Computers configured in workgroups have only local accounts. You might also need to log on locally to a domain computer to administer it. Only users with a local user account can log on locally. When you log on locally, you have access to any resource on the computer that your account or the groups to which your account belongs are granted access.

Managing User Account Control and Elevation Prompts

User Account Control (UAC) represents a significant change in the way in which user accounts are used and configured. It affects which privileges standard users and administrator users have, how applications are installed and run, and much more. In this section, I'll extend the discussion in Chapter 1, "Introduction to Windows 7 Administration," and provide a comprehensive look at how UAC affects user and administrator accounts. This is essential information to know when managing Windows 7 systems.

> ***NOTE*** **Learning how UAC works will help you be a better administrator. To support UAC, many aspects of the Windows operating system had to be reworked. Some of the most extensive changes have to do with how applications are installed and run. In Chapter 9, "Installing and Maintaining Programs," you'll find a complete discussion of how the architectural changes affect programs running on Windows 7.**

Redefining Standard User and Administrator User Accounts

In Windows XP and earlier versions of Windows, malicious software programs can exploit the fact that most user accounts are configured as members of the local computer's Administrators group. Not only does this allow malicious software to install itself, but it also allows malicious software to use these elevated privileges to wreak havoc on the computer, because programs installed by administrators can write to otherwise secure areas of the registry and the file system.

To combat the growing threat of malicious software, organizations have locked down computers, required users to log on using standard user accounts, and required administrators to use the Run As command to perform administrative tasks. Unfortunately, these procedural changes can have serious negative consequences on productivity. A person logged on as a standard user under Windows XP can't perform some of the most basic tasks, such as changing the system clock and calendar, changing the computer's time zone, or changing the computer's power management settings. Many software programs designed for Windows XP simply will not function properly without local administrator rights—these programs use local administrator rights to write to system locations during installation and during normal operations. Additionally, Windows XP doesn't let you know beforehand when a task you are performing requires administrator privileges.

UAC seeks to improve usability while at the same time enhancing security by redefining how standard user and administrator user accounts are used. UAC represents a fundamental shift in computing by providing a framework that limits the scope of administrator-level access privileges and requires all applications to run in a specific user mode. In this way, UAC prevents users from making inadvertent changes to system settings and locks down the computer to prevent unauthorized applications from being installed or performing malicious actions.

Because of UAC, Windows 7 defines two levels of user accounts: standard and administrator. Windows 7 also defines two modes (run levels) for applications: standard user mode and administrator mode. Although standard user accounts can use most software and can change system settings that do not affect other users or the security of the computer, administrator user accounts have complete access to the computer and can make any changes that are needed. When an administrator user starts an application, her access token and its associated administrator privileges are applied to the application, giving her all the rights and privileges of a local computer administrator for that application. When a standard user starts an application, her access token and its associated privileges are applied to the application at run time, limiting her to the rights and privileges of a standard user for that application. Further, all applications are configured to run in a specific mode during installation. Any tasks run by standard-mode applications that require administrator privileges not only are identified during setup but require user approval to run.

In Windows 7, the set of privileges assigned to standard user accounts has changed. Tasks that standard user accounts can perform include:

- Installing fonts, viewing the system clock and calendar, and changing the time zone.
- Changing the display settings and the power management settings.
- Adding printers and other devices (when the required drivers are installed on the computer or are provided by an IT administrator).
- Downloading and installing updates (when the updates use UAC-compatible installers).
- Creating and configuring virtual private network (VPN) connections. VPN connections are used to establish secure connections to private networks over the public Internet.
- Installing Wired Equivalent Privacy (WEP) to connect to secure wireless networks. The WEP security protocol provides wireless networks with improved security.

Windows 7 also defines two run levels for applications: standard and administrator. Windows 7 determines whether a user needs elevated privileges to run a program by supplying most applications and processes with a security token. If an application has a standard token, or an application cannot be identified as an administrator application, elevated privileges are not required to run the application, and Windows 7 starts it as a standard application by default. If an application has an administrator token, elevated privileges are required to run the application, and Windows 7 prompts the user for permission or confirmation prior to running the application.

The process of getting approval prior to running an application in administrator mode and prior to performing tasks that change system configuration is known as *elevation.* Elevation enhances security and reduces the impact of malicious software by notifying users before they perform any action that could impact system settings and by preventing applications from using administrator privileges without first notifying users. Elevation also protects administrator applications from attacks by standard applications. For more information on elevation and how UAC works with applications, see Chapter 9.

By default, Windows 7 switches to the secure desktop prior to displaying the elevation prompt. The secure desktop restricts the programs and processes that have access to the desktop environment, and in this way reduces the possibility that a malicious program or user could gain access to the process being elevated. If you don’t want Windows 7 to switch to the secure desktop prior to prompting for elevation, you can choose settings that use the standard desktop rather than the secure desktop. However, this makes the computer more susceptible to malware and attack.

Optimizing User Account Control and Admin Approval Mode

Every computer has a built-in local Administrator account. This built-in account is not protected by UAC, and using this account for administration can put your computer at risk. To safeguard computers in environments in which you use a local Administrator account for administration, you should create a new local Administrator account and use this account for administration.

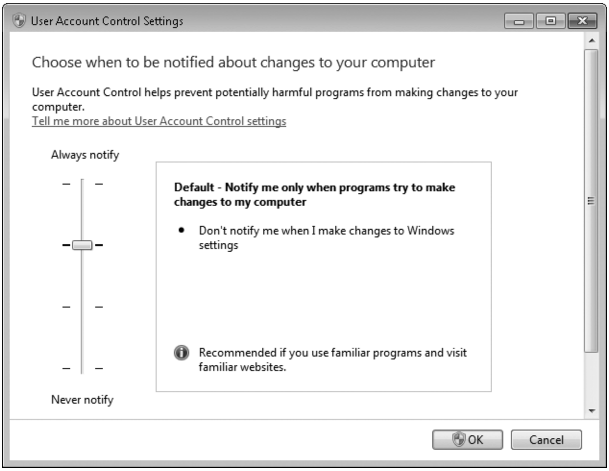
UAC can be configured or disabled for any individual user account. If you disable UAC for a user account, you lose the additional security protections UAC offers and put the computer at risk. To completely disable UAC or to reenable UAC after disabling it, the computer must be restarted for the change to take effect.

Admin Approval Mode is the key component of UAC that determines whether and how administrators are prompted when running administrator applications. The default way that Admin Approval Mode works is as follows:

- All administrators, including the built-in local Administrator account, run in and are subject to Admin Approval Mode.
- Because they are running in and subject to Admin Approval Mode, all administrators, including the built-in local Administrator account, see the elevation prompt when they run administrator applications.

If you are logged on as an administrator, you can modify the way UAC works for all users by completing the following steps:

1. In Control Panel, click System And Security. Under the Action Center heading, click Change User Account Control Settings.
2. On the User Account Control Settings page, shown in Figure 5-1, use the slider to choose when to be notified about changes to the computer, and then click OK. Table 5-1 summarizes the available options.



User Account Control Settings

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.

Tell me more about User Account Control settings

Always notify

Default - Notify me only when programs try to make changes to my computer

- Don't notify me when I make changes to Windows settings

Recommended if you use familiar programs and visit familiar websites.

Never notify

FIGURE 5-1 The User Account Control Settings page

TABLE 5-1 User Account Control Settings

OPTION	DESCRIPTION	WHEN TO USE	USES THE SECURE DESKTOP?
Always Notify	Always notifies the current user when programs try to install software or make changes to the computer and when the user changes Windows settings.	Choose this option when a computer requires the highest security possible and users frequently install software and visit unfamiliar Web sites.	Yes
Default	Notifies the current user only when programs try to make changes to the computer and not when the user changes Windows settings.	Choose this option when a computer requires high security and you want to reduce the number of notification prompts that users see.	Yes
Notify Me Only When … (Do Not Dim My Desktop)	Same as Default but also prevents UAC from switching to the secure desktop.	Choose this option when users work in a trusted environment with familiar applications and do not visit unfamiliar Web sites.	No

OPTION	DESCRIPTION	WHEN TO USE	USES THE SECURE DESKTOP?
Never Notify	Turns off all UAC notification prompts.	Choose this option when security is not a priority and users work in a trusted environment with programs that are not certified for Windows 7 because they do not support UAC.	No

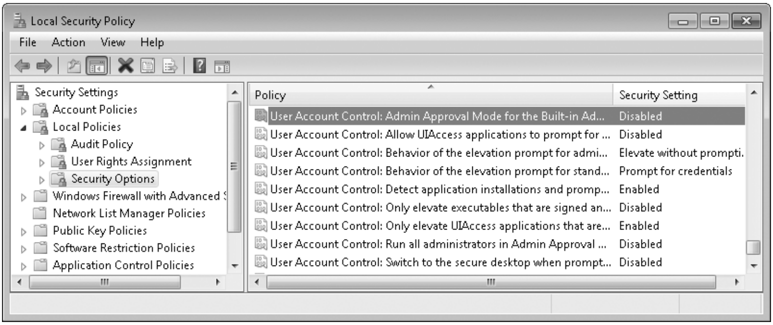
In Group Policy, you can manage Admin Approval Mode and elevation prompting by using settings under Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options. These security settings are:

- **User Account Control: Admin Approval Mode For The Built-In Administrator Account** Determines whether users and processes running as the built-in local Administrator account are subject to Admin Approval Mode. By default, this feature is enabled, which means the built-in local Administrator account is subject to Admin Approval Mode and also subject to the elevation prompt behavior stipulated for administrators in Admin Approval Mode. If you disable this setting, users and processes running as the built-in local administrator are not subject to Admin Approval Mode and therefore not subject to the elevation prompt behavior stipulated for administrators in Admin Approval Mode.
- **User Account Control: Allow UIAccess Applications To Prompt For Elevation Without Using The Secure Desktop** Determines whether User Interface Accessibility (UIAccess) programs can automatically disable the secure desktop for elevation prompts used by a standard user. If you enable this setting, UIAccess programs, including Windows Remote Assistance, can disable the secure desktop for elevation prompts.
- **User Account Control: Behavior Of The Elevation Prompt For Administrators In Admin Approval Mode** Determines whether administrators subject to Admin Approval Mode see an elevation prompt when running administrator applications, and also determines how the elevation prompt works. By default, administrators are prompted for consent when running administrator applications on the secure desktop. You can configure this option so that administrators are prompted for consent without the secure desktop, prompted for credentials with or without the secure desktop (as is the case with standard users), or prompted for consent only for non-Windows binaries. You can also configure this option so that administrators are not prompted at all, in which case an administrator will be elevated automatically. No setting will prevent an administrator from right-clicking an application shortcut and selecting Run As Administrator.

- **User Account Control: Behavior Of The Elevation Prompt For Standard Users** Determines whether users logged on with a standard user account see an elevation prompt when running administrator applications. By default, users logged on with a standard user account are prompted for the credentials of an administrator on the secure desktop when running administrator applications or performing administrator tasks. You can also configure this option so that users are prompted for credentials on the standard desktop rather than the secure desktop, or you can deny elevation requests automatically, in which case users will not be able to elevate their privileges by supplying administrator credentials. The latter option doesn't prevent users from right-clicking an application shortcut and selecting Run As Administrator.
- **User Account Control: Run All Administrators In Admin Approval Mode** Determines whether users logged on with an administrator account are subject to Admin Approval Mode. By default, this feature is enabled, which means administrators are subject to Admin Approval Mode and also subject to the elevation prompt behavior stipulated for administrators in Admin Approval Mode. If you disable this setting, users logged on with an administrator account are not subject to Admin Approval and therefore are not subject to the elevation prompt behavior stipulated for administrators in Admin Approval Mode.
- **User Account Control: Only Elevate UIAccess Applications That Are Installed in Secure Locations** Determines whether UIAccess programs must reside in a secure location on the file system to elevate. If enabled, UIAccess programs must reside in a secure location under %SystemRoot%\Program Files, %SystemRoot%\Program Files(x86), or %SystemRoot%\Windows\System32.
- **User Account Control: Only Elevate Executables That Are Signed And Validated** Determines whether applications must be signed and validated to elevate. If enabled, only executables that pass signature checks and have certificates in the Trusted Publisher store will elevate. Use this option only when the highest security is required and you've verified that all applications in use are signed and valid.

In a domain environment, you can use Active Directory–based Group Policy to apply the security configuration you want to a particular set of computers. You can also configure these settings on a per-computer basis using local security policy. To do this, follow these steps:

1. Click Start, point to All Programs, Administrative Tools, and then click Local Security Policy.
2. In the Local Security Policy console tree, under Security Settings, expand Local Policies, and then select Security Options, as shown in Figure 5-2.



Policy	Security Setting
User Account Control: Admin Approval Mode for the Built-in Ad...	Disabled
User Account Control: Allow UIAccess applications to prompt for ...	Disabled
User Account Control: Behavior of the elevation prompt for admi...	Elevate without prompti.
User Account Control: Behavior of the elevation prompt for stand...	Prompt for credentials
User Account Control: Detect application installations and promp...	Enabled
User Account Control: Only elevate executables that are signed an...	Disabled
User Account Control: Only elevate UIAccess applications that are...	Enabled
User Account Control: Run all administrators in Admin Approval ...	Disabled
User Account Control: Switch to the secure desktop when prompt...	Disabled

FIGURE 5-2 The Local Security Policy console

3. Double-click the setting you want to work with, make any necessary changes, and then click OK. Repeat this step to modify other security settings as necessary.

Managing Local Logon

All local computer accounts should have passwords. If an account is created without a password, anyone can log on to the account, and there is no protection for the account. However, a local account without a password cannot be used to remotely access a computer.

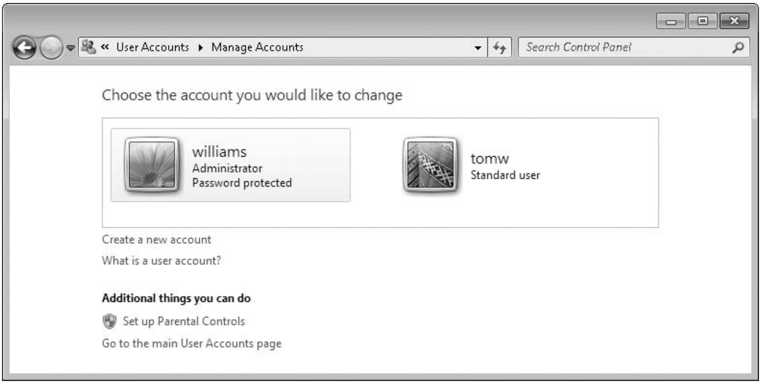
The sections that follow discuss how to create and work with local user accounts. Every workstation computer has local computer accounts, whether the computer is a member of a homegroup, a workgroup, or a domain.

Creating Local User Accounts in a Homegroup or Workgroup

For a computer that is a member of a homegroup or a workgroup, you can create a local user account by following these steps:

1. In Control Panel, under the User Accounts heading, click Add Or Remove User Accounts. This displays the Manage Accounts page.

   As Figure 5-3 shows, the Manage Accounts page lists all configurable user accounts on the local computer by account type and with configuration details. If an account has a password, it is labeled Password Protected. If an account is disabled, it is listed as being off.
2. Click Create A New Account. This displays the Create New Account page.
3. Type the name of the local account. This name is displayed on the Welcome screen and Start menu.
4. Set the type of account as either Standard User or Administrator. To give the user full permissions on the local computer, select Administrator.
5. Click Create Account.



Choose the account you would like to change

williams
Administrator
Password protected

tomw
Standard user

Create a new account

What is a user account?

Additional things you can do

Set up Parental Controls

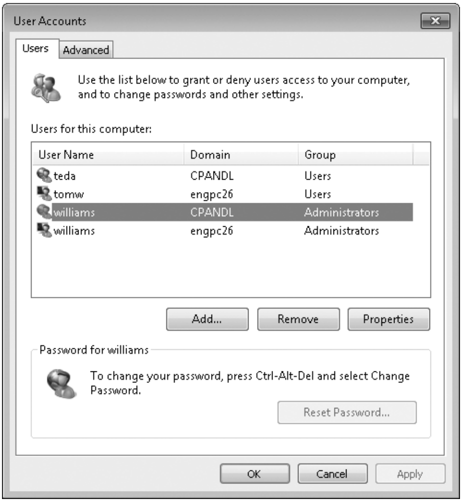
Go to the main User Accounts page

FIGURE 5-3 In a homegroup or workgroup, use the Manage Accounts page in Control Panel to add or remove local user accounts.

Granting Access to an Existing Domain Account to Allow Local Logon

If a user needs to be able to log on locally to a computer and has an existing domain account, you can grant the user permission to log on locally by completing the following steps:

1. In Control Panel, under the User Accounts heading, click the Change Account Type link. This displays the User Accounts dialog box. As Figure 5-4 shows, the User Accounts dialog box lists all configurable user accounts on the local computer by domain and with group membership details.



Use the list below to grant or deny users access to your computer, and to change passwords and other settings.

Users for this computer:

User Name	Domain	Group
teda	CPANDL	Users
tomw	engpc26	Users
williams	CPANDL	Administrators
williams	engpc26	Administrators

Password for williams

To change your password, press Ctrl-Alt-Del and select Change Password.

FIGURE 5-4 Use the User Accounts dialog box to manage local user accounts on a computer that is a member of a domain.

2. Click Add. This starts the Add New User wizard.
3. You are creating a local computer account for a user with an existing domain account. Type the user's domain account name and domain in the fields provided.
4. Using the options provided, select the type of user account.
5. A standard user account is created as a member of the local Users group. To give the user the permissions of a normal user, select Standard User.
6. An administrator account is created as a member of the local Administrators group. To give the user full permissions on the local computer, select Administrator.
7. An Other account is created as a member of a group you specify. To give the user the permissions of a specific group, select Other, and then select the group.
8. Click Finish. If you need to set other permissions or add the user to other local groups, follow the steps specified in the section "Managing Local User Accounts and Groups."

Changing Local User Account Types

The User Accounts utility provides an easy way to change account types for local users. You can also quickly set one of the default account types. For more advanced control, however, you need to use Local Users And Groups to assign group membership to individual accounts. (See the section "Adding and Removing Local Group Members.")

In a homegroup or workgroup, you can change the account type for a local computer user by completing the following steps:

1. In Control Panel, under the User Accounts heading, click Add Or Remove User Accounts. This displays the Manage Accounts page.
2. Click the account you want to change, and then click Change The Account Type.
3. On the Change Account Type page, set the level of access for the user as either Standard User or Administrator, and then click Change The Account Type.

In a domain, you can change the account type for a local computer user by completing the following steps:

1. In Control Panel, click User Accounts. On the User Accounts page, click Change Account Type. This displays the User Accounts dialog box.
2. On the Users tab, click the user account you want to work with, and then click Properties.
3. In the Properties dialog box, click the Group Membership tab.

4. Set the type of account as Standard User or Administrator, or select Other and then select the group you want to use.
5. Click OK twice.

Creating Passwords for Local User Accounts

In a homegroup or workgroup configuration, local user accounts are created without passwords by default. This means that a user can log on simply by clicking his account name on the Welcome screen or by clicking OK on the classic Log On To Windows screen. To improve security, all local accounts should have passwords.

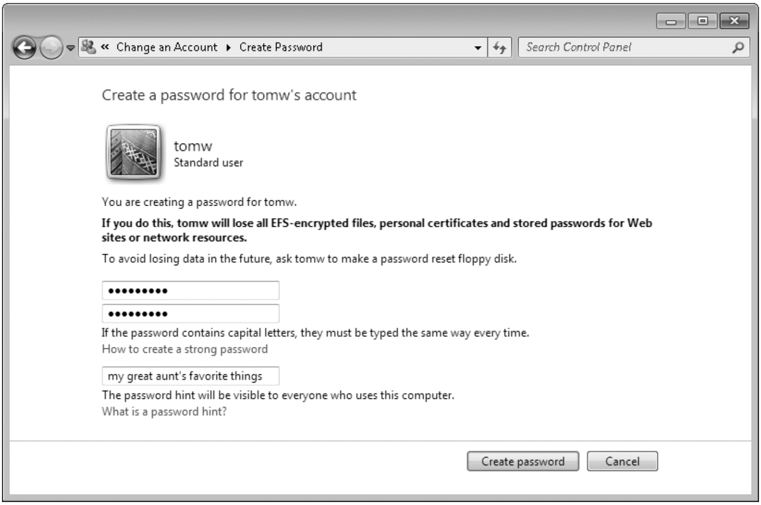
For the easiest management of local accounts, log on to each account that should have a password, and then use the User Accounts utility to assign a password to the account. If you are logged on as the user when you create a password, you don't have to worry about losing encrypted data. If you create a password without logging on as the user, the user will lose access to his or her encrypted files, encrypted e-mail, personal certificates, and stored passwords. This occurs because the user's master key, which is needed to access his or her personal encryption certificate and unlock this data, is encrypted with a hash that is based on an empty password. So when you create a password, the hash doesn't match, and there's no way to unlock the encrypted data. The only way to resolve this is to restore the original settings by removing the password from the account. The user should then be able to access his or her encrypted files. Again, this issue is related only to local user accounts for computers and not to domain user accounts.

> ***TIP*** **Only the User Accounts utility allows you to assign a password hint, which can be helpful in recovering a forgotten or lost password. Another technique for recovering a password is a password reset disk, which can be a floppy disk or a USB flash drive. It is important to note that these are the only techniques you should use to recover passwords for local user accounts unless you want to risk data loss. Why? Although you can create, reset, or remove a password from a user account, doing so deletes any personal certificates and stored passwords associated with this account. As a result, the user will no longer be able to access his or her encrypted files or private e-mail messages that have been encrypted with his or her personal key. In addition, he or she will lose stored passwords for Web sites and network resources. It is also important to note that this is an issue only for local user accounts. Administrators can change or reset passwords for domain user accounts without affecting access to encrypted data.**

You can create a password for a local user account by completing the following steps:

1. Log on as the user whose password you want to create. In Control Panel, under the User Accounts heading, click Add Or Remove User Accounts. This displays the Manage Accounts page.

2. Click the account you want to work with. To prevent possible data loss, this should be the same account as the account with which you logged on. Any account that has a current password is listed as Password Protected. Any account without this label doesn't have a password.
3. Click Create A Password. Type a password, and then confirm it, as illustrated in Figure 5-5. Afterward, type a unique password hint. The password hint is a word or phrase that can be used to obtain the password if it is lost or forgotten. This hint is visible to anyone who uses the computer.



Create a password for tomw's account

tomw
Standard user

You are creating a password for tomw.

If you do this, tomw will lose all EFS-encrypted files, personal certificates and stored passwords for Web sites or network resources.

To avoid losing data in the future, ask tomw to make a password reset floppy disk.

••••••••••

••••••••••

If the password contains capital letters, they must be typed the same way every time.

How to create a strong password

my great aunt's favorite things

The password hint will be visible to everyone who uses this computer.

What is a password hint?

FIGURE 5-5 Create a password with a password hint.

4. Click Create Password.

Recovering Local User Account Passwords

As discussed previously, in order to preserve access to any encrypted data and stored passwords that a user might have, it is preferable to try and recover a user password rather than change or remove the password.

Windows 7 provides two ways to recover user passwords:

- **Password hint** A hint can be accessed on the Welcome screen. Ordinarily, the Welcome screen is displayed when the computer is started and no one is logged on. If someone is logged on to the workstation, ask him or her to log off. Click the user's name to display the Password prompt, and then click the blue enter button to display the password hint. Hopefully, the password hint will help the user remember the password. If it doesn't, you need to use a password reset disk.

- **Password reset disk** Password reset disks can be created for any local user account with a password. They enable anyone to change the password of the related local account without needing to know the old password. Because anyone with access to these disks can change account passwords, you should store password reset disks in a secure location. If users are allowed to create their own password reset disks, be sure they know how important the disks are.

NOTE **Passwords for domain users and those for local users are managed differently. Administrators manage passwords for domain user accounts and can reset forgotten passwords using the Active Directory Users And Computers console.**

Passwords for local machine accounts can be stored in a secure, encrypted file on a password reset disk, which can be a floppy disk or a USB flash device. You can create a password reset disk for the current user as discussed in "Creating and Using a Password Reset Disk" in Chapter 1. You can reset a password for a local machine account as discussed in "Resetting a User's Password" in Chapter 1.

Controlling Logon: Welcome Screens and Classic Logons

By default, Windows 7 displays a Welcome screen when a computer is part of a homegroup or workgroup. Windows displays a Logon screen when a computer is part of a domain. The difference between the Welcome screen and the Logon screen is an important one.

In a homegroup or workgroup, the Welcome screen is displayed when no one is logged on or when the screen saver is activated and you attempt to log on again. On the Welcome screen, you see a list of accounts on the computer. To log on with one of these accounts, click the account and type a password if required. Contrary to what many people think, the Welcome screen doesn't display all the accounts that have been created on the computer. Some accounts, such as Administrator, are hidden from view automatically.

The Welcome screen is convenient because it displays a list of available accounts and enables you to log on by clicking an account name. To enhance security in a homegroup or workgroup by not giving a list of accounts, you can use the Logon screen instead of the Welcome screen. In a domain, the Logon screen is displayed automatically when no one is logged on or when the screen saver is activated and you attempt to log on again. The Logon screen requires users to type a logon name rather than selecting an account from a list of available accounts.

The Logon screen has several features that you can control. By default, the name of the last user to log on is displayed in the User Name field of the Log On To Windows dialog box. Hiding the user name of the last user to log on can improve security by requiring users to know a valid account name for the computer. To do this, start the Local Security Policy tool from the Administrative Tools menu or type **secpol.msc** at an elevated command prompt. Then, under Local Policies\Security

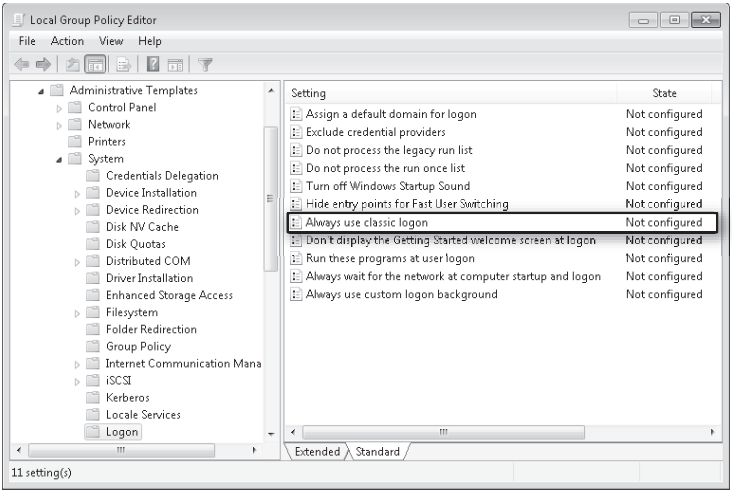
Options, double-click Interactive Logon: Do Not Display Last User Name. Click Enabled, and then click OK.

You can configure whether the Welcome screen is used through the Always Use Classic Logon setting in Group Policy. You have the following options:

- Enable the policy to use the Logon screen rather than the Welcome screen.
- Disable the policy to use the Welcome screen.
- Use Not Configured to use the default configuration (the Welcome screen).

In a domain environment, you can use Active Directory–based Group Policy to apply the security configuration you want to a particular set of computers. You can also configure this setting on a per-computer basis by using local security policy. To configure a homegroup or workgroup computer to use the Logon screen rather than the Welcome screen, use the Group Policy Object Editor, which is an MMC snap-in. You can add this snap-in to an empty console and configure a computer to use the Logon screen by following these steps:

1. Click Start, type **gpedit.msc**, and then press Enter. This opens the Local Group Policy Editor with the top-level Local Group Policy object open for editing.
2. In the editor, expand Local Computer Policy, Computer Configuration, Administrative Templates, System, Logon. (See Figure 5-6.)



- Administrative Templates
  - Control Panel
  - Network
  - Printers
  - System
    - Credentials Delegation
    - Device Installation
    - Device Redirection
    - Disk NV Cache
    - Disk Quotas
    - Distributed COM
    - Driver Installation
    - Enhanced Storage Access
    - Filesystem
    - Folder Redirection
    - Group Policy
    - Internet Communication Mana
    - iSCSI
    - Kerberos
    - Locale Services
    - Logon

Setting	State
Assign a default domain for logon	Not configured
Exclude credential providers	Not configured
Do not process the legacy run list	Not configured
Do not process the run once list	Not configured
Turn off Windows Startup Sound	Not configured
Hide entry points for Fast User Switching	Not configured
Always use classic logon	Not configured
Don't display the Getting Started welcome screen at logon	Not configured
Run these programs at user logon	Not configured
Always wait for the network at computer startup and logon	Not configured
Always use custom logon background	Not configured

11 setting(s)

FIGURE 5-6 Enable the Always Use Classic Logon setting to use the Logon screen rather than the Welcome screen.

3. Double-click Always Use Classic Logon.
4. Select Enabled, and then click OK.

In a domain, by default you cannot bypass the requirement to press Ctrl+Alt+Del to access the Log On To Windows dialog box. You can eliminate this requirement, but it is a poor security practice. To do so, in the Local Security Policy tool, expand Local Policies\Security Options, and then double-click Interactive Logon: Do Not Require Ctrl+Alt+Del. Click Enabled, and then click OK.

Removing Accounts and Denying Local Access to Workstations

Domain administrators are automatically granted access to local resources on workstations. Other users aren't granted access to local resources on workstations other than to the computers to which they are permitted to log on. As workstations are moved around an organization, you might find that previous owners of a workstation still have access to its resources or that users who were granted temporary access to a workstation were never removed from the access list.

In a domain, you can control the workstations to which users can log on by using the account properties in Active Directory Users And Computers. Double-click the account to display the Properties dialog box. On the Account tab, click the Log On To button.

In a homegroup or workgroup, you can remove a user's local account and effectively deny logon by completing these steps:

1. Log on as a user with local administrator privileges. In Control Panel, under the User Accounts heading, click Add Or Remove User Accounts. This displays the Manage Accounts page.
2. Click the account you want to remove.
3. Click Delete The Account.
4. Before deleting the account, you have the opportunity save the contents of the user's desktop and documents folders to a folder on the current user's desktop. To save the user's desktop and documents, click Keep Files. To delete the files, click Delete Files.
5. Confirm the account deletion by clicking Delete Account.

   Keep in mind that in a domain, unless further restrictions are in place with regard to logging on to a workstation, a user might still be able to gain access to the workstation by logging on with a domain account.

Managing Stored Credentials

In Windows 7, you can use Credential Manager to store credentials that can be used to try to automatically log on users to servers, Web sites, and programs. Credentials are stored in an electronic vault (called the Windows vault) that provides easy logon to essential resources, wherever they might be located. If you find that a user frequently has problems logging on to protected resources, such as the company intranet or an external Internet site, you can create a stored credential for each resource that the user works with.

Credential Manager supports three types of stored credentials:

- **Windows credential** A credential that uses standard Windows authentication (NTLM or Kerberos) and includes a resource location, logon account name, and password.
- **Certificate-based credential** A credential that includes a resource location and uses a certificate saved in the Personal store in Certificate Manager for authentication.
- **Generic credential** A credential that uses basic or custom authentication techniques and includes a resource location, logon account name, and password.

The following sections examine techniques for working with stored credentials.

Adding Windows or Generic Credentials

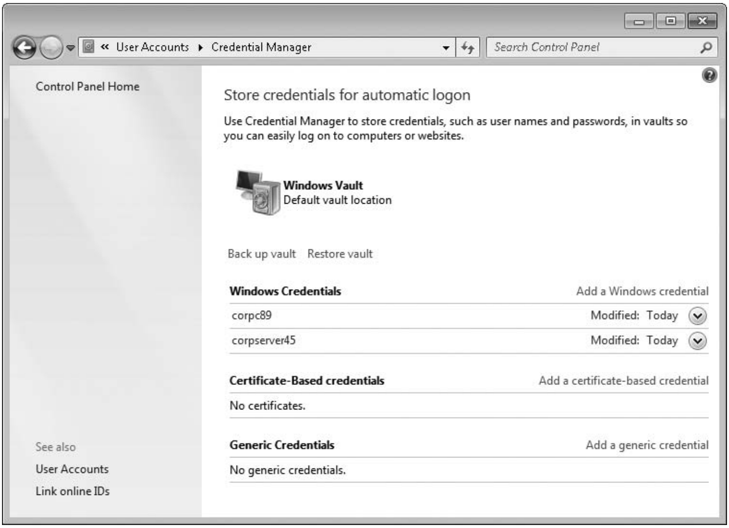
Each user account has a unique Windows vault. Entries in the Windows vault are stored in the user's profile settings and contain information needed to log on to protected resources. If you are logged on to a domain account when you create a Windows vault entry, and the account has a roaming profile (instead of a local or mandatory profile), the information stored in the Windows vault entry is available when you log on to any computer in the domain. Otherwise, the information in the Windows vault entry is available only on the computer on which you create the entry.

REAL WORLD **When your organization has computers that are in workgroups or homegroups rather than part of your domain, you'll find that stored credentials can save everyone a lot of time. For example, if Ted uses a computer that is a member of a workgroup for his daily activities but needs to access several different servers in several different locations or domains, you can make this process easier by creating a Windows credential for each resource. Now, no matter how Ted accesses the servers, he can be authenticated automatically and without having to provide alternate credentials. For example, if Ted maps a network drive to FileServer84 and you've set up a credential for this server, Ted doesn't have to select the Connect Using Different Credential option and then provide alternate credentials.**

To add an entry to the current logged-on user's Windows vault, follow these steps:

1. Log on as the user whose Windows vault entries you want to manage. In Control Panel, click User Accounts, and then click Credential Manager.

   On the Credential Manager page, shown in Figure 5-7, you'll see a list of current entries by credential type (if there are any credentials).



Store credentials for automatic logon

Use Credential Manager to store credentials, such as user names and passwords, in vaults so you can easily log on to computers or websites.

Windows Vault
Default vault location

Back up vault   Restore vault

Windows Credentials	Add a Windows credential
corpc89	Modified: Today
corpserver45	Modified: Today

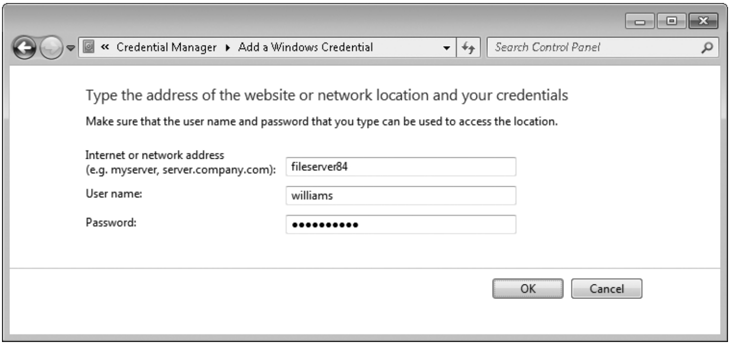
Certificate-Based credentials	Add a certificate-based credential
No certificates.	

Generic Credentials	Add a generic credential
No generic credentials.	

FIGURE 5-7 Review the currently available credentials and options.

2. Click Add A Windows Credential or Add A Generic Credential as appropriate for the type of credential you are creating. Then use the options provided to configure the credential (as shown in Figure 5-8). The available fields are as follows:
   - **Internet Or Network Address** The network or Internet resource for which you are configuring the Windows vault entry. This can be a server name, such as fileserver86; a fully qualified domain name for an Internet resource, such as www.microsoft.com; or an address containing a wildcard, such as *.microsoft.com. When you use a server name or fully qualified domain name, the entry is used for accessing a specific server or service. When you use a wildcard, the entry is used for any server in the specified domain. For example, the entry *.microsoft.com could be used to access *www.microsoft.com*, *ftp.microsoft.com*, *smtp.microsoft.com*, and *extranet.microsoft.com*.
   - **User Name** The user name required by the server, including any necessary domain qualifiers. To use the default domain for a resource, enter only the user name, such as Williams. For a nondefault domain, type the full domain and account name, such as technology\Williams. For an Internet service, type the full service account name, such as Williams@msn.com.
   - **Password** The password required by the server. One of the things most users forget is that whenever they change their password on the server or service, they must also change their password in their Windows vault. If a user forgets to change the password in the Windows vault, repeated

attempts to log on or connect to the server or service might result in the account being locked.



Type the address of the website or network location and your credentials

Make sure that the user name and password that you type can be used to access the location.

Internet or network address (e.g. myserver, server.company.com): fileserver84

User name: williams

Password: ••••••••••

FIGURE 5-8 Create the Windows vault entry by setting the necessary logon information.

4. Click OK to save the credential.

Adding Certificate-Based Credentials

The Personal certificate store in the user's profile stores certificates that have been issued to authenticate the user. Once you've added a certificate for the user, you can create a credential that uses the certificate to access a resource.

To add an entry for a certificate-based credential to the currently logged-on user's Windows vault, follow these steps:

1. Log on as the user whose Windows vault entries you want to manage. In Control Panel, click User Accounts, and then click Credential Manager.
2. On the Credential Manager page, you'll see a list of current entries by credential type (if there are any credentials).
3. Click Add A Certificate-Based Credential. In the Internet Or Network Address field, enter the name of the network or Internet resource for which you are configuring the Windows vault entry. This can be a server name, a fully qualified domain name for an Internet resource, or an address containing a wildcard.
4. Click Select Certificate. In the Select Certificate dialog box, click the personal certificate that you want to use for the resource, and then click OK.
5. Click OK again to save the credential.

Editing Windows Vault Entries

You can edit Windows vault entries at any time, but keep in mind that local Windows vault entries are visible only on the computer on which they were created. This means that if you want to modify an entry, you must log on to the local workstation where the entry was created. The only exception is for users with roaming profiles. When a user has a roaming profile, Windows vault entries can be edited from any computer where the user is logged on.

Use the following steps to edit a user's Windows vault entries:

1. Log on as the user whose Windows vault entries you want to manage. In Control Panel, click User Accounts, and then click Credential Manager.

   On the Credential Manager page, you'll see a list of current entries by credential type.
2. Click the credential entry that you want to edit.
3. Click Edit.
4. As necessary, specify new values for the user name and password or the certificate associated with the credential, and then click Save.

Backing Up and Restoring the Windows Vault

You can back up a user's stored credentials by backing up the Windows vault. After you back up the Windows vault, you can restore the credentials or transfer them to a new computer simply by restoring the Windows vault. In most cases, you should back up the Windows vault to removable media.

To back up a user's Windows vault, follow these steps:

1. Log on as the user whose Windows vault entries you want to manage. In Control Panel, click User Accounts, and then click Credential Manager.

   On the Credential Manager page, you'll see a list of current entries by credential type.
2. Click Back Up Vault.
3. On the Stored User Names And Passwords page, click Browse. Use the Save Backup File As dialog box to select a save location and specify a name for the credential backup file. Credential backup files are saved with the .crd file extension. Click Save.
4. Click Next. Press Ctrl+Alt+Delete to switch to the secure desktop. When prompted, enter and confirm a password for the credential backup file.
5. Click Next, and then click Finish.

To restore a user's Windows vault on the same or different computer, follow these steps:

1. Log on as the user whose Windows vault entries you want to manage. In Control Panel, click User Accounts, and then click Credential Manager.
2. On the Credential Manager page, click Restore Vault.

3. On the Stored User Names And Passwords page, click Browse. Use the Open Backup File As dialog box to select the location and file in which you saved the credential backup files, and then click Open.
4. Click Next. Press Ctrl+Alt+Delete to switch to the secure desktop. When prompted, enter the password for the credential backup file.
5. Click Next, and then click Finish.

Removing Windows Vault Entries

When a user no longer needs a Windows vault entry, you should remove it. To remove a user's Windows vault entry, follow these steps:

1. Log on as the user whose Windows vault entries you want to manage. In Control Panel, click User Accounts, and then click Credential Manager.

   On the Credential Manager page, you'll see a list of current entries by credential type.
2. Click the credential entry that you want to remove.
3. Click Remove From Vault. When prompted to confirm the action, click Yes.

As stated previously, local Windows vault entries can be removed only on the computer on which they were created. When a user has a roaming profile, however, Windows vault entries can be deleted from any computer to which the user is logged on.

Managing Local User Accounts and Groups

Local user accounts and groups are managed much like domain accounts. You can create accounts, manage their properties, reset accounts when they are locked or disabled, and so on. In addition to being able to manage local user accounts with Control Panel, you can create local user accounts with Local Users And Groups or with policy preferences. You should:

- Use Local Users And Groups to manage local user accounts on one computer.
- Use policy preferences to manage local user accounts on multiple computers throughout a domain.

When working with policy preferences, you can manage users and groups through Computer Configuration entries or User Configuration entries. Use Computer Configuration if you want to configure preferences that should be applied to computers regardless of who logs on. Use User Configuration if you want to configure preferences that should be applied to users regardless of which computer they log on to.

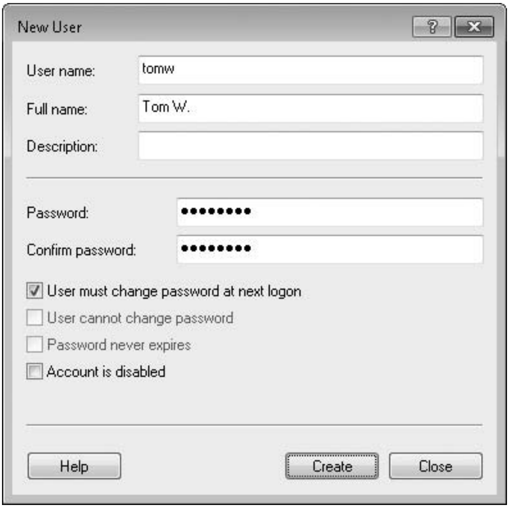
Creating Local User Accounts

You can access Local Users And Groups and create a user account by completing the following steps:

1. Click Start, point to All Programs, Administrative Tools, and then click Computer Management. Alternatively, open Control Panel, click System And Security, scroll down, click Administrative Tools, and then double-click Computer Management.
2. Right-click the Computer Management entry in the console tree, and then click Connect To Another Computer on the shortcut menu. You can now select the Windows 7 workstation whose local accounts you want to manage. (Domain controllers do not have local users or groups.)
3. Under the System Tools node, double-click the Local Users And Groups node to expand it, and then select Users. In the details pane, you should see a list of the currently defined user accounts.
4. Right-click Users, and then click New User. This opens the New User dialog box, shown in Figure 5-9.

   The fields in the dialog box are used as follows:

   - **User Name** The logon name for the user account. This name should follow the conventions for the local user name policy.
   - **Full Name** The full name of the user, such as William R. Stanek.
   - **Description** A description of the user. Normally, you would type the user's job title, such as Webmaster. You could also type the user's job title and department.
   - **Password** The password for the account. This password should follow the conventions of your password policy.
   - **Confirm Password** A field to ensure that you assign the account password correctly. Simply retype the password to confirm it.
   - **User Must Change Password At Next Logon** If this check box is selected, the user must change the password upon logon.
   - **User Cannot Change Password** If this check box is selected, the user can't change the password.
   - **Password Never Expires** If this check box is selected, the password for this account never expires. This setting overrides the local account policy.
   - **Account Is Disabled** If this check box is selected, the account is disabled and can't be used. Use this field to temporarily prevent anyone from using an account.



New User

User name: tomw

Full name: Tom W.

Description:

Password: •••••••••

Confirm password: •••••••••

☑ User must change password at next logon

□ User cannot change password

□ Password never expires

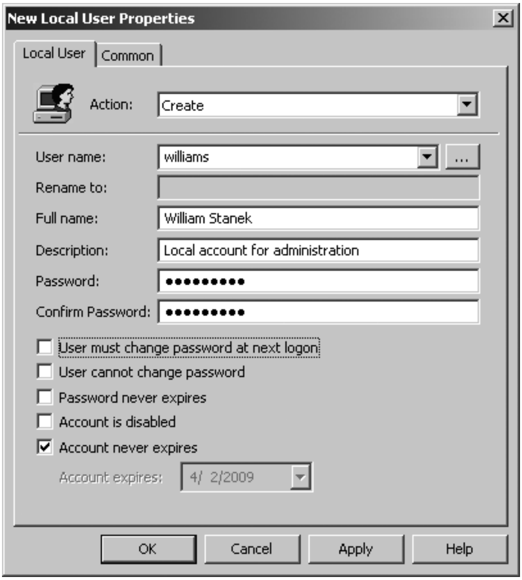
□ Account is disabled

FIGURE 5-9 Configure new workstation accounts using the New User dialog box in Local Users And Groups.

5. Click Create when you have finished configuring the new account.

You can access Group Policy and use a preference item to create a user account by completing the following steps:

1. Open a Group Policy object (GPO) for editing in the Group Policy Management Editor. To configure preferences for computers, expand Computer Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups. To configure preferences for users, expand User Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups.
2. Right-click the Local Users And Groups node, point to New, and then select Local User. This opens the New Local User Properties dialog box, shown in Figure 5-10.
3. In the Action list, select Create. The rest of the fields in the dialog box are used as described in the previous procedure.
4. Use the options on the Common tab to control how the preference is applied. In most cases, you'll want to create the new account only once. If so, select Apply Once And Do Not Reapply.
5. Click OK. The next time Group Policy is refreshed, the preference item will be applied as appropriate for the Group Policy object in which you defined the preference item.



Action: Create

User name: williams

Rename to:

Full name: William Stanek

Description: Local account for administration

Password: ●●●●●●●●●

Confirm Password: ●●●●●●●●●

□ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account is disabled

☑ Account never expires

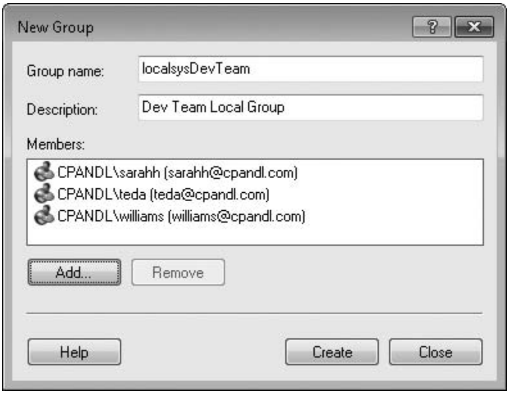
Account expires: 4/ 2/2009

FIGURE 5-10 Configure new local user accounts in Group Policy.

Creating Local Groups for Workstations

You create local groups with Local Users And Groups or with Group Policy. You can access Local Users And Groups and create a local group by completing the following steps:

1. Click Start, point to All Programs, Administrative Tools, and then click Computer Management. Alternatively, open Control Panel, click System And Security, scroll down, click Administrative Tools, and then double-click Computer Management.
2. Right-click the Computer Management entry in the console tree, and then click Connect To Another Computer on the shortcut menu. You can now select the Windows 7 workstation whose local accounts you want to manage. (Domain controllers do not have local users or groups.)
3. Under the System Tools node, double-click the Local Users And Groups node to expand it, and then select Groups. In the details pane, you should see a list of the currently defined group accounts.
4. Right-click Groups, and then select New Group. This opens the New Group dialog box, shown in Figure 5-11.



Group name: localsysDevTeam

Description: Dev Team Local Group

Members:

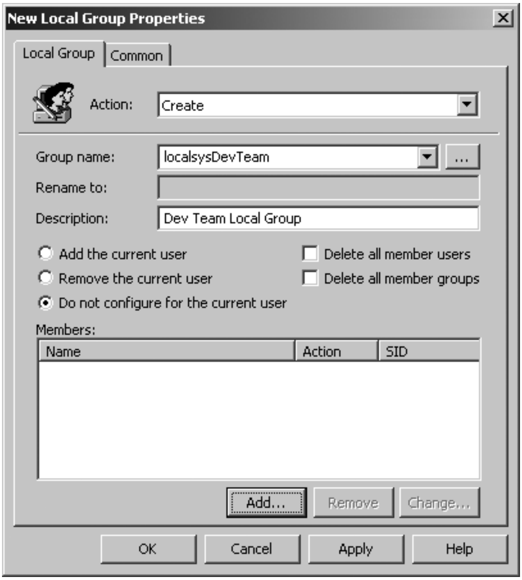
CPANDL\sarahh (sarahh@cpandl.com)
CPANDL\teda (teda@cpandl.com)
CPANDL\williams (williams@cpandl.com)

FIGURE 5-11 The New Group dialog box enables you to add a new local group to a Windows 7 workstation.

5. After you type a name and description for the group, click the Add button to open the Select Users dialog box and add names to the group.
6. In the Select Users dialog box, click Locations to select the computer or domain in which the user accounts you want to work with are located.
7. Type the name of a user you want to use in the Enter The Object Names To Select field, and then click Check Names. If matches are found, select the account you want to use, and then click OK. If no matches are found, update the name you entered and try searching again. Repeat this step as necessary, and then click OK when you have finished.
8. The New Group dialog box is updated to reflect your selections. If you made a mistake, select a name and remove it by clicking Remove.
9. Click Create when you have finished adding or removing group members.

You can access Group Policy and use a preference item to create a local group by completing the following steps:

1. Open a Group Policy object (GPO) for editing in the Group Policy Management Editor. To configure preferences for computers, expand Computer Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups. To configure preferences for users, expand User Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups.
2. Right-click the Local Users And Groups node, point to New, and then select Local Group. This opens the New Local Group Properties dialog box, shown in Figure 5-12.



New Local Group Properties

Action: Create

Group name: localsysDevTeam

Rename to:

Description: Dev Team Local Group

○ Add the current user

○ Remove the current user

● Do not configure for the current user

□ Delete all member users

□ Delete all member groups

Members:

Name	Action	SID

FIGURE 5-12 Configure new local group accounts in Group Policy.

3. In the Action list, select Create. Enter a name and description for the group.
4. Specify whether the current user should be added or removed as a member of the group, or select Do Not Configure For The Current User.
5. To add members to the group, click Add. In the Local Group Member dialog box, click the browse button (the one with the three dots). Use the Select User, Computer Or Group dialog box to select a user or group to add to the local group, and then click OK twice. Repeat this step as necessary.
6. Use the options on the Common tab to control how the preference is applied. In most cases, you should create the new account only once. If so, select Apply Once And Do Not Reapply.
7. Click OK. The next time Group Policy is refreshed, the preference item will be applied as appropriate for the Group Policy object in which you defined the preference item.

Adding and Removing Local Group Members

You use Local Users And Groups to add or remove local group members. Complete the following steps:

1. Expand Local Users And Groups in Computer Management, and then select the Groups folder in the left pane. Double-click the group with which you want to work.

2. Click the Add button to add user accounts to the group. This opens the Select Users dialog box. In the Select Users dialog box, type the name of a user you want to use in the Enter The Object Names To Select field, and then click Check Names. If matches are found, select the account you want to use, and then click OK. If no matches are found, update the name you entered and try searching again. Repeat this step as necessary, and then click OK.
3. Use the Remove button to remove user accounts from the group. Simply select the user account you want to remove from the group, and then click Remove.
4. Click OK when you have finished.

You can access Group Policy and use a preference item to add or remove members from a local group by completing the following steps:

1. Open a Group Policy object (GPO) for editing in the Group Policy Management Editor. To configure preferences for computers, expand Computer Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups. To configure preferences for users, expand User Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups.
2. Right-click the Local Users And Groups node, point to New, and then select Local Group. This opens the New Local Group Properties dialog box.
3. In the Action list, select Update to update the group's settings, or select Replace to delete the group and then re-create it exactly as you specify. If you update a group, you can enter a new name in the Rename To box.
4. Specify whether the current user should be added or removed as a member of the group, or select Do Not Configure For The Current User.
5. Specify whether all existing member users, all existing member groups, or both should be deleted.
6. To add or remove group members, click Add. In the Local Group Member dialog box, in the Action list, select Add To This Group if you are adding a member, or select Remove From This Group if you are removing a member. Next, click the browse button (the one with the three dots). Use the Select User, Computer Or Group dialog box to select a user or group to add to the local group, and then click OK twice. Repeat this step as necessary.
7. Use the options on the Common tab to control how the preference is applied, and then click OK. The next time policy is refreshed, the preference item will be applied as appropriate for the Group Policy object in which you defined the preference item.

Enabling or Disabling Local User Accounts

Local user accounts can become disabled for several reasons. If a user forgets his password and tries to guess it, he might exceed the account policy for bad logon attempts. Another administrator could have disabled the account while a user was on vacation. When an account is disabled or locked out, you can enable it by using the methods described here.

When an account is disabled, you can enable it on a local computer by completing the following steps:

1. Expand Local Users And Groups in Computer Management, and then select the Users folder in the left pane.
2. In the right pane, double-click the user's account name, and then clear the Account Is Disabled check box.
3. Click OK.

When an account is locked out, you can enable it on a local computer by completing the following steps:

1. In Local Users And Groups, select the Users folder in the left pane.
2. In the right pane, double-click the user's account name, and then clear the Account Is Locked Out check box.
3. Click OK.

You can enable or disable accounts and set other account options through policy preferences by completing the following steps:

1. Open a Group Policy object (GPO) for editing in the Group Policy Management Editor. To configure preferences for computers, expand Computer Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups. To configure preferences for users, expand User Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups.
2. In the right pane, double-click the user's account name to open the related Properties dialog box.
3. Select Update in the Action list. Make any necessary changes, and then click OK. The next time policy is refreshed, the preference item will be applied as appropriate for the Group Policy object in which you defined the preference item.

Creating a Secure Guest Account

In some environments, you might need to set up a Guest account that can be used by visitors. Most of the time, you'll want to configure the Guest account on a specific computer or computers and carefully control how the account can be used. To create a secure Guest account, I recommend that you perform the following tasks:

- **Enable the Guest account for use.** By default, the Guest account is disabled, so you must enable it to make it available. To do this, access Local Users And Groups in Computer Management, and then select the Users folder. Double-click Guest, and then clear the Account Is Disabled check box. Click OK.

- **Set a secure password for the Guest account.** By default, the Guest account has a blank password. To improve security on the computer, you should set a password for the account. In Local Users And Groups, right-click Guest, and then select Set Password. Click Proceed at the warning prompt. Type the new password and then confirm it. Click OK twice.
- **Ensure that the Guest account cannot be used over the network.** The Guest account shouldn't be accessible from other computers. If it is, users at another computer could log on over the network as a guest. To prevent this, start the Local Security Policy tool from the Administrative Tools menu, or type **secpol.msc** at the command prompt. Then, under Local Policies\User Rights Assignment, check that the Deny Access To This Computer From The Network policy lists Guest as a restricted account.
- **Prevent the Guest account from shutting down the computer.** When a computer is shutting down or starting up, it is possible that a guest user (or anyone with local access) could gain unauthorized access to the computer. To help deter this, you should be sure that the Guest account doesn't have the Shut Down The System user right. In the Local Security Policy tool, expand Local Policies\User Rights Assignment, and ensure that the Shut Down The System policy doesn't list the Guest account.
- **Prevent the Guest account from viewing event logs.** To help maintain the security of the system, the Guest account shouldn't be allowed to view the event logs. To be sure this is the case, start Registry Editor by typing **regedit** at a command prompt, and then access the HKLM\SYSTEM\CurrentControlSet\services\Eventlog key. Here, among others, you'll find three important subkeys: Application, Security, and System. Make sure each of these subkeys has a DWORD value named RestrictGuestAccess with a value of 1.

Renaming Local User Accounts and Groups

When you rename an account, you give it a new label. Because the SID for the account remains the same, the permissions and properties associated with the account don't change. To rename an account while you are accessing a local computer, complete the following steps:

1. In Local Users And Groups, select the Users or Groups folder, as appropriate.
2. Right-click the account name, and then click Rename. Type the new account name, and then click a different entry.

To rename an account using Group Policy, complete the following steps:

1. Open a Group Policy object (GPO) for editing in the Group Policy Management Editor. To configure preferences for computers, expand Computer Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups. To configure preferences for users, expand User Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups.

2. Do one of the following:
   - If a preference item already exists for the user or group, double-click the user or group name to open the related Properties dialog box. Select Update in the Action list. In the Rename To box, type the new account name, and then click OK.
   - If a preference item doesn't already exist for the user or group, you need to create one using the techniques discussed previously. Because you want to rename the user or group, select Update in the Action list, and then type the new account name in the Rename To box.

Deleting Local User Accounts and Groups

Deleting an account permanently removes it. Once you delete an account, if you create another account with the same name, you can't automatically get the same permissions because the SID for the new account won't match the SID for the account you deleted.

Because deleting built-in accounts can have far-reaching effects on the workstation, Windows 7 doesn't let you delete built-in user accounts or group accounts. In Local Users And Groups, you can remove other types of accounts by selecting them and pressing the Delete key or by right-clicking and then clicking Delete. When prompted, click Yes.

> ***NOTE*** **When you delete a user account using Local Users And Groups, Windows 7 doesn't delete the user's profile, personal files, or home directory. If you want to delete these files and directories, you have to do it manually.**

To delete an account using Group Policy, complete the following steps:

1. Open a Group Policy object (GPO) for editing in the Group Policy Management Editor. To configure preferences for computers, expand Computer Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups. To configure preferences for users, expand User Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups.
2. Do one of the following:
   - If a preference item already exists for the user or group, double-click the user or group name to open the related Properties dialog box. Select Delete in the Action list. On the Common tab, set the appropriate options, such as Apply Once And Do Not Reapply, and then click OK.
   - If a preference item doesn't already exist for the user or group, you need to create one for the user or group using the techniques discussed previously. Be sure to select Delete in the Action list, and then select the appropriate options on the Common tab.

Managing Remote Access to Workstations

Windows 7 has several remote connectivity features. With Remote Assistance, users can send invitations to support technicians, enabling the technicians to service a computer remotely. With Remote Desktop, users can connect remotely to a computer and access its resources. In this section, you'll learn how to configure Remote Assistance and Remote Desktop. Typically, neither the Remote Assistance feature nor the Remote Desktop feature is enabled, and you must enable these features manually.

Remote Assistance and Remote Desktop can function through Network Address Translation (NAT) firewalls. Remote Assistance also has built-in diagnostic tools. To allow for easier troubleshooting and escalation of support issues, two different support staff can connect to a remote computer simultaneously. When troubleshooting requires restarting the computer, Remote Assistance sessions are reestablished automatically after the computer being diagnosed reboots.

Prior to using Remote Assistance, you may want users to use the Problem Steps Recorder to create a step-by-step record of a problem they are experiencing. The Problem Steps Recorder is very easy to use. To start and use the Problem Steps Recorder, a user needs to complete the following steps:

1. To start the Problem Steps Recorder, have the user click Start, type **psr**, and then press Enter. Once the tool is started, the user can prepare the environment and then begin recording the problem.
2. To turn on recording, the user clicks Start Record. Once recording has started, the user can perform the action that isn't working and click Add Comment to add comments as she works.
3. When the user experiences the problem and the related errors have been displayed, she can stop recording by clicking Stop Record.
4. When the user stops recording, the Save As dialog box is displayed. The user selects a save location and name for the Zip file that contains the record of the problem in an .mht file.
5. The user can send the Zip file to a support technician in an e-mail message or by copying it to a file share. To review the recorded problem steps, you double-click the Zip file to display its contents in Windows Explorer and then double-click the enclosed .mht file to open it in Internet Explorer.
6. You'll then see screen captures for all the steps the user took while the problem was being recorded. After the screen captures, you'll find additional details for each step that are generated automatically. You can use this information along with any user comments to help you troubleshoot the problem.

Configuring Remote Assistance

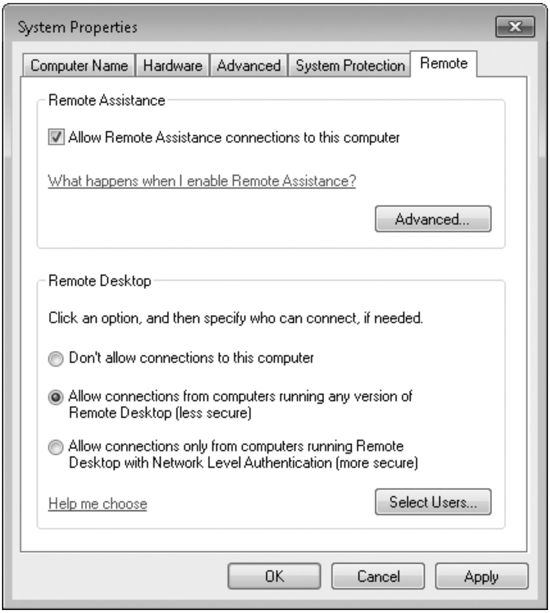
Remote Assistance is a useful feature for help desks, whether in-house or outsourced. A user can allow support personnel to view and take control of his or her desktop. This feature can be used to walk users through a complex process or to manage system settings while they watch the progress of the changes. The key to Remote Assistance is in the access levels you grant.

When enabled, Remote Assistance is configured by default to let support personnel view and control computers. Because users can send assistance invitations to internal and external resources, this could present a security concern for organizations. To reduce potential security problems, you might want to allow support staff to view but not control computers. A new restriction for Windows 7 is to allow connections only from computers running Windows 7 or later. This option is helpful to limit any possible compatibility issues and to ensure that any security enhancements in Windows 7 or later operating systems are available within Remote Assistance sessions.

Another key aspect of Remote Assistance you can control is the time limit for invitations. The default maximum time limit is 6 hours; the absolute maximum time limit you can assign is 30 days. Although the intent of a multiple-day invitation is to give support personnel a time window in which to respond to requests, it also means that they could use an invitation to access a computer over a period of 30 days. For instance, suppose you send an invitation with a 30-day time limit to a support person who resolves the problem the first day. That person would still have access to the computer for another 29 days, which wouldn't be desirable for security reasons. To reduce the risk to your systems, you'll usually want to reduce the default maximum time limit considerably—say, to 1 hour. If the problem is not solved in the allotted time period, you can issue another invitation.

To configure Remote Assistance, follow these steps:

1. In Control Panel, click System And Security, and then click System.
2. On the System page, click Remote Settings in the left pane. This opens the System Properties dialog box with the Remote tab displayed, as shown in Figure 5-13.
3. To disable Remote Assistance, clear the Allow Remote Assistance Connections To This Computer check box, and then click OK. Skip the remaining steps.
4. To enable Remote Assistance, select Allow Remote Assistance Connections To This Computer.



Remote Assistance

☑ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Remote Desktop

Click an option, and then specify who can connect, if needed.

○ Don't allow connections to this computer

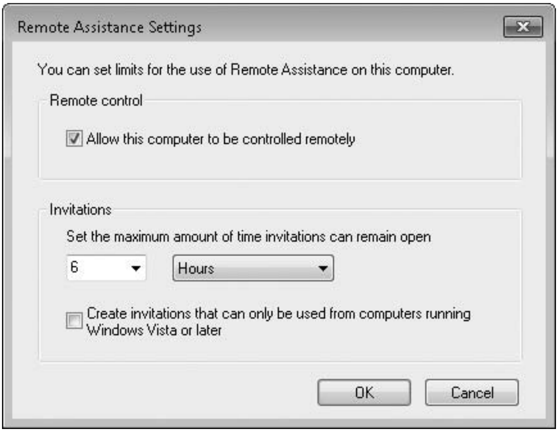
● Allow connections from computers running any version of Remote Desktop (less secure)

○ Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)

Help me choose

FIGURE 5-13 Use the Remote tab options to configure remote access to the computer.

5. Click Advanced. This displays the Remote Assistance Settings dialog box, shown in Figure 5-14.



You can set limits for the use of Remote Assistance on this computer.

Remote control

☑ Allow this computer to be controlled remotely

Invitations

Set the maximum amount of time invitations can remain open

6 Hours

□ Create invitations that can only be used from computers running Windows Vista or later

FIGURE 5-14 The Remote Assistance Settings dialog box is used to set limits for Remote Assistance.

6. The Allow This Computer To Be Controlled Remotely option sets limits for Remote Assistance. When selected, this setting allows assistants to view and control the computer. To provide view-only access to the computer, clear this check box.
7. The Invitations options control the maximum time window for invitations. You can set a value in minutes, hours, or days, up to a maximum of 30 days. If you set a maximum limit value of 10 days, for example, a user can create an invitation with a time limit up to but not more than 10 days. The default maximum expiration limit is 6 hours.
8. Click OK twice when you have finished configuring Remote Assistance options.

In Group Policy, you can manage Remote Assistance using the policy settings shown in Table 5-2. These settings are found in the Administrative Templates policies for Computer Configuration under the paths shown.

TABLE 5-2 Policy Settings for Managing Remote Assistance

SETTING	PATH
Allow Only Vista Or Later Connections	\System\Remote Assistance
Do Not Allow Windows Messenger To Be Run	\Windows Components\Windows Messenger
Offer Remote Assistance	\System\Remote Assistance
Solicited Remote Assistance	\System\Remote Assistance
Turn On Session Logging	\System\Remote Assistance

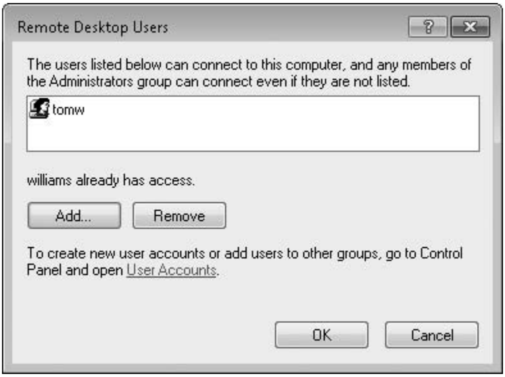
Configuring Remote Desktop Access

Unlike Remote Assistance, which provides only a view of the current user's desktop, Remote Desktop provides several levels of access:

- If a user is logged on to the desktop locally and then tries to log on remotely, the local desktop locks, and the user can access all of the running applications just as though he or she were sitting at the keyboard. This feature is useful for users who want to work from home or other locations outside the office, enabling them to continue to work with applications and documents that they were using prior to leaving the office.
- If a user is listed on the workstation's Remote Access list and is not otherwise logged on, he or she can initiate a new Windows session. The Windows session behaves as though the user were sitting at the keyboard. It can even be used when other users are also logged on to the computer. In this way, multiple users can share a single workstation and use its resources.

Remote Desktop is not enabled by default. You must specifically enable it to allow remote access to the workstation. When it is enabled, any member of the Administrators group can connect to the workstation. Other users must be placed on a remote access list to gain access to the workstation. To configure remote access, follow these steps:

1. In Control Panel, click System And Security, and then click System.
2. On the System page, click Remote Settings in the left pane. This opens the System Properties dialog box to the Remote tab.
3. To disable Remote Desktop, select Don't Allow Connections To This Computer, and then click OK. Skip the remaining steps.
4. To enable Remote Desktop, you have two options. You can:
   - Select Allow Connections From Computers Running Any Version Of Remote Desktop to allow connections from any version of Windows.
   - Select Allow Connections Only From Computers Running Remote Desktop With Network Level Authentication to allow connections only from Windows 7 or later computers (and computers with secure network authentication).
5. Click Select Users. This displays the Remote Desktop Users dialog box, shown in Figure 5-15.



Remote Desktop Users

The users listed below can connect to this computer, and any members of the Administrators group can connect even if they are not listed.

tomw

williams already has access.

To create new user accounts or add users to other groups, go to Control Panel and open User Accounts.

FIGURE 5-15 Specify the additional users allowed to make Remote Desktop connections.

6. To grant Remote Desktop access to a user, click Add. This opens the Select Users dialog box. In the Select Users dialog box, click Locations to select the computer or domain in which the users you want to work with are located. Type the name of a user you want to work with in the Enter The Object Names To Select field, and then click Check Names. If matches are found, select the account you want to use and then click OK. If no matches are

found, update the name you entered and try searching again. Repeat this step as necessary, and then click OK.

7. To revoke remote access permissions for a user account, select the account and then click Remove.
8. Click OK twice when you have finished.

Windows Firewall must be configured to allow inbound Remote Desktop exceptions. You can configure this on a per-computer basis in Windows Firewall for the domain profile and the standard profile. In Group Policy, you can configure this exception and manage Remote Desktop by using the policy settings shown in Table 5-3. These settings are found in the Administrative Templates policies for Computer Configuration under the path shown.

TABLE 5-3 Policy Settings for Managing Remote Desktop

SETTING	COMPUTER CONFIGURATION PATH
	PATHS UNDER WINDOWS COMPONENTS\ REMOTE DESKTOP SERVICES
Allow .Rdp Files From Unknown Publishers	\Remote Desktop Connection Client
Allow .Rdp Files From Valid Publishers And User's Default .Rdp Settings	\Remote Desktop Connection Client
Always Prompt For Password Upon Connection	\Remote Desktop Session Host\ Security
Automatic Reconnection	\Remote Desktop Session Host\ Connections
Configure Server Authentication For Client	\Remote Desktop Connection Client
Deny Logoff Of An Administrator Logged In To The Console Session	\Remote Desktop Session Host\ Connections
Do Not Allow Local Administrators To Customize Permissions	\Remote Desktop Session Host\ Security
Do Not Allow Passwords To Be Saved	\Remote Desktop Connection Client
Limit Maximum Color Depth	\Remote Desktop Session Host\ Remote Session Environment
Limit Maximum Display Resolution	\Remote Desktop Session Host\ Remote Session Environment
Limit Maximum Number Of Monitors	\Remote Desktop Session Host\ Remote Session Environment

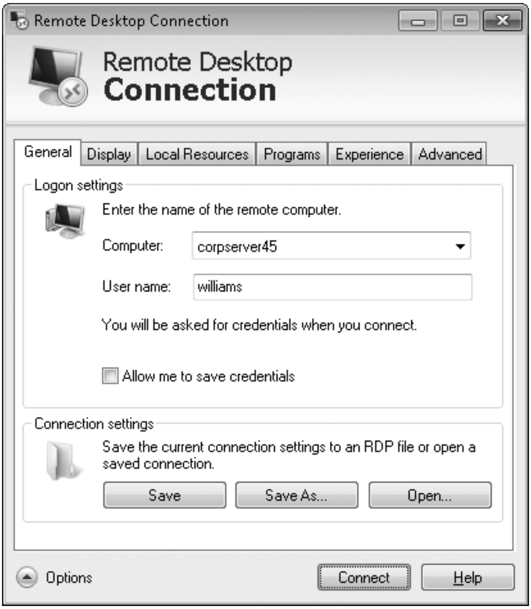
SETTING	COMPUTER CONFIGURATION PATH
Limit The Size Of The Entire Roaming User Profile Cache	\Remote Desktop Session Host\Profiles
Require Use Of Specific Security Layer For Remote (Rdp) Connections	\Remote Desktop Session Host\Security
Set Client Connection Encryption Level	\Remote Desktop Session Host\Security
Set Compression Algorithm For Rdp Data	\Remote Desktop Session Host\Remote Session Environment
Specify Sha1 Thumbprints Of Certificates Representing Trusted .Rdp Publishers	\Remote Desktop Connection Client
	OTHER PATHS
Disable Remote Desktop Sharing	\Windows Components\NetMeeting
Windows Firewall: Allow Inbound Remote Desktop Exceptions	\Network\Network Connections\Windows Firewall\Domain Profile
Windows Firewall: Allow Inbound Remote Desktop Exceptions	\Network\Network Connections\Windows Firewall\Standard Profile

Making Remote Desktop Connections

As an administrator, you can make Remote Desktop connections to Windows servers and workstations. With Windows 2000 Server, Remote Desktop connections are enabled by installing Terminal Services and then configuring Terminal Services in remote access mode. With Windows XP Professional and later versions, Remote Desktop is installed automatically, but it is normally not enabled until you do so as discussed in the preceding section of this chapter. Once remote access is enabled on a computer, all administrators have remote access to that computer. Other users can be granted remote access as well.

To make a Remote Desktop connection to a server or workstation, follow these steps:

1. At a command prompt, type **mstsc**, or click Start, point to All Programs, Accessories, and then click Remote Desktop Connection. Click the Options button. This displays the Remote Desktop Connection dialog box, shown in Figure 5-16.



Logon settings

Enter the name of the remote computer.

Computer: corpserver45

User name: williams

You will be asked for credentials when you connect.

□ Allow me to save credentials

Connection settings

Save the current connection settings to an RDP file or open a saved connection.

FIGURE 5-16 In the Remote Desktop Connection dialog box, type the name of the computer to which you want to connect, and then click Connect.

2. In the Computer field, type the name of the computer to which you want to connect. If you don't know the name of the computer, use the drop-down list to choose an available computer, or select Browse For More in the drop-down list to display a list of domains and computers in those domains.
3. Specify additional options as necessary. If you've configured stored credentials for the computer, your saved credentials will be used automatically. You can edit or delete the credentials as necessary.
4. Click Connect. If you haven't previously stored credentials for the computer, type your credentials when prompted, and then click OK. If the connection is successful, you'll see the Remote Desktop window on the selected computer, and you'll be able to work with resources on the computer. In the case of a failed connection, check the information you provided and then try to connect again.

NOTE **Clicking Options in the Remote Desktop Connection dialog box displays additional options for creating and saving connections. These options enable you to change the display size for the Remote Desktop, manage connections to local resources (such as printers, serial ports, and disk drives), run programs automatically on connection, and enable or disable local caching and data compression.**

CHAPTER 9

Installing and Maintaining Programs

Administrators and support staff often install and configure applications that are used on desktop computers. You need to install and configure applications before deploying new computers, install new applications on computers when the programs are requested, and update applications when new versions become available. Also, as users install additional applications, you might be called on to help troubleshoot installation problems or to help uninstall programs. Most program installation problems are fairly easy to solve if you know what to look for. Other problems are fairly difficult to resolve and require more work than you might expect. In this chapter, you'll learn how User Account Control (UAC) affects how you install and run applications and about techniques for installing, uninstalling, and maintaining programs.

Managing Application Virtualization and Run Levels

User Account Control (UAC) changes the way that applications are installed and run, where applications write data, and what permissions applications have. In this section, I'll look at how UAC affects application installation, from application security tokens to file and registry virtualization to run levels. This information is essential when you are installing and maintaining applications on Windows 7.

Application Access Tokens and Location Virtualization

All applications used with Windows 7 are divided into two general categories:

- **UAC-compliant** Any application written specifically for Windows Vista or Windows 7 is considered a compliant application. Applications certified as complying with the Windows 7 architecture have the UAC-compliant logo.
- **Legacy** Any application written for Windows XP or an earlier version of Windows is considered a legacy application.

The distinction between UAC-compliant applications and legacy applications is important because of the architectural changes required to support UAC. UAC-compliant applications use UAC to reduce the attack surface of the operating system. They do this by preventing unauthorized programs from installing or running without the user's consent and by restricting the default privileges granted to applications. These measures make it harder for malicious software to take over a computer.

> ***NOTE*** **The Windows 7 component responsible for UAC is the Application Information service. This service facilitates the running of interactive applications with an "administrator" access token. You can see the difference between the administrator user and standard user access tokens by opening two Command Prompt windows, running one with elevation (right-click, and then click Run As Administrator), and the other as a standard user. In each window, type whoami /all and compare the results. Both access tokens have the same security identifiers (SIDs), but the elevated, administrator user access token will have more privileges than the standard user access token.**

All applications that run on Windows 7 derive their security context from the current user's access token. By default, UAC turns all users into standard users even if they are members of the Administrators group. If an administrator user consents to the use of her administrator privileges, a new access token is created for the user. It contains all the user's privileges, and this access token—rather than the user's standard access token—is used to start an application or process.

In Windows 7, most applications can run using a standard user access token. Whether applications need to run with standard or administrator privileges depends on the actions the application performs. Applications that require administrator privileges, referred to as *administrator user applications,* differ from applications that require standard user privileges, referred to as *standard user applications,* in the following ways:

- Administrator user applications require elevated privileges to run and perform core tasks. Once started in elevated mode, an application with a user's administrator access token can perform tasks that require administrator privileges and can also write to system locations of the registry and the file system.

- Standard user applications do not require elevated privileges to run or to perform core tasks. Once started in standard user mode, an application with a user's standard access token must request elevated privileges to perform administration tasks. For all other tasks, the application should not run using elevated privileges. Further, the application should write data only to nonsystem locations of the registry and the file system.

Applications not written for Windows 7 run with a user's standard access token by default. To support the UAC architecture, these applications run in a special compatibility mode and use file system and registry virtualization to provide "virtualized" views of file and registry locations. When an application attempts to write to a system location, Windows 7 gives the application a private copy of the file or registry value. Any changes are then written to the private copy, and this private copy is then stored in the user's profile data. If the application attempts to read or write to this system location again, it is given the private copy from the user's profile to work with. By default, if an error occurs when the application is working with virtualized data, the error notification and logging information show the virtualized location rather than the actual location that the application was trying to work with.

Application Integrity and Run Levels

The focus on standard user and administrator privileges also changes the general permissions required to install and run applications. In Windows XP and earlier versions of Windows, the Power Users group gave users specific administrator privileges to perform basic system tasks when installing and running applications. Applications written for Windows 7 do not require the use of the Power Users group. Windows 7 maintains it only for legacy application compatibility.

As part of UAC, Windows 7 by default detects application installations and prompts users for elevation to continue the installation. Installation packages for UAC-compliant applications use application manifests that contain run-level designations to help track required privileges. Application manifests define the application's privileges as one of the following:

- **RunAsInvoker** Run the application with the same privileges as the user. Any user can run the application. For a standard user or a user who is a member of the Administrators group, the application runs with a standard access token. The application runs with higher privileges only if the parent process from which it is started has an administrator access token. For example, if you open an elevated Command Prompt window and then launch an application from this window, the application runs with an administrator access token.
- **RunAsHighest** Run the application with the highest privileges of the user. The application can be run by both administrator users and standard users. The tasks the application can perform depend on the user's privileges. For a standard user, the application runs with a standard access token. For a user who is a member of a group with additional privileges, such as the Backup

Operators, Server Operators, or Account Operators group, the application runs with a partial administrator access token that contains only the privileges the user has been granted. For a user who is a member of the Administrators group, the application runs with a full administrator access token.

- **RunAsAdmin** Run the application with administrator privileges. Only administrators can run the application. For a standard user or a user who is a member of a group with additional privileges, the application runs only if the user can be prompted for credentials required to run in elevated mode or if the application is started from an elevated process, such as an elevated Command Prompt window. For a user who is a member of the Administrators group, the application runs with an administrator access token.

To protect application processes, Windows 7 labels them with integrity levels ranging from high to low. Applications that modify system data, such as Disk Management, are considered high integrity. Applications performing tasks that could compromise the operating system, such as Windows Internet Explorer 8 in Windows 7, are considered low integrity. Applications with lower integrity levels cannot modify data in applications with higher integrity levels.

Windows 7 identifies the publisher of any application that attempts to run with an administrator's full access token. Then, depending on that publisher, Windows 7 marks the application as belonging to one of the following three categories:

- Windows Vista / Windows 7
- Publisher verified (signed)
- Publisher not verified (unsigned)

To help you quickly identify the potential security risk of installing or running the application, a color-coded elevation prompt displays a particular message depending on the category to which the application belongs:

- If the application is from a blocked publisher or is blocked by Group Policy, the elevation prompt has a red background and displays the message "The application is blocked from running."
- If the application is administrative (such as Computer Management), the elevation prompt has a blue-green background and displays the message "Windows needs your permission to continue."
- If the application has been signed by Authenticode and is trusted by the local computer, the elevation prompt has a gray background and displays the message "A program needs your permission to continue."
- If the application is unsigned (or is signed but not yet trusted), the elevation prompt has a yellow background and red shield icon and displays the message "An unidentified program wants access to your computer."

Prompting on the secure desktop can be used to further secure the elevation process. The secure desktop safeguards the elevation process by preventing spoofing of the elevation prompt. The secure desktop is enabled by default in Group

Policy, as discussed in the section “Optimizing User Account Control and Admin Approval Mode” in Chapter 5.

Setting Run Levels

By default, only applications running with a user’s administrator access token run in elevated mode. Sometimes, you’ll want an application running with a user’s standard access token to be in elevated mode. For example, you might want to start the Command Prompt window in elevated mode so that you can perform administration tasks.

In addition to application manifests (discussed in the previous section), Windows 7 provides two different ways to set the run level for applications:

- Run an application once as an administrator.
- Always run an application as an administrator.

To run an application once as an administrator, right-click the application’s shortcut or menu item, and then click Run As Administrator. If you are using a standard account and prompting is enabled, you are prompted for consent before the application is started. If you are using a standard user account and prompting is disabled, the application will fail to run. If you are using an administrator account and prompting for consent is enabled, you are prompted for consent before the application is started.

Windows 7 also enables you to mark an application so that it always runs with administrator privileges. This approach is useful for resolving compatibility issues with legacy applications that require administrator privileges. It is also useful for UAC-compliant applications that normally run in standard mode but that you use to perform administration tasks. As examples, consider the following:

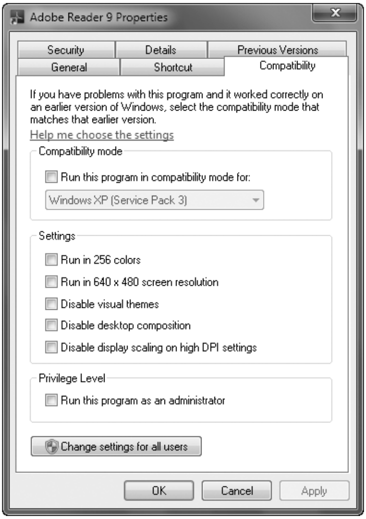
- A standard application written for Windows 7 is routinely run in elevated mode and used for administration tasks. To eliminate the need to right-click the application shortcut and choose Run As Administrator before running the application, you can mark it to always run as an administrator.
- An application written for Windows XP or an earlier version of Windows requires administrator privileges. Because this program is configured to use standard mode by default under Windows 7, the program isn’t running properly and is generating numerous errors. To resolve the compatibility problem, you could create an application compatibility shim using the Windows Application Compatibility Toolkit (ACT) version 5.5 or later. As a temporary solution, you can mark the application to always run as an administrator.

NOTE **You cannot mark system applications or processes to always run with administrator privileges. Only nonsystem applications and processes can be marked to always run at this level.**

REAL WORLD **The Windows Application Compatibility Toolkit (ACT) is a solution for administrators that requires no reprogramming of an application. ACT can help you resolve common compatibility problems. For example, some programs run only on a specific operating system or when the user is an administrator. Using ACT, you can create a shim that responds to the application inquiry about the operating system or user level with a True statement, which allows the application to run. ACT also can help you create more in-depth solutions for applications that try to write to protected areas of the operating system or use elevated privileges when they don't need to. ACT can be downloaded from the Microsoft Download Center (*http://download.microsoft.com*).**

You can mark an application to always run as an administrator by following these steps:

1. On the Start menu, locate the program that you want to always run as an administrator.
2. Right-click the application's shortcut, and then click Properties.
3. In the Properties dialog box, click the Compatibility tab, shown in Figure 9-1.



Adobe Reader 9 Properties

If you have problems with this program and it worked correctly on an earlier version of Windows, select the compatibility mode that matches that earlier version.

Help me choose the settings

Compatibility mode

□ Run this program in compatibility mode for:

Windows XP (Service Pack 3)

Settings

□ Run in 256 colors

□ Run in 640 x 480 screen resolution

□ Disable visual themes

□ Disable desktop composition

□ Disable display scaling on high DPI settings

Privilege Level

□ Run this program as an administrator

FIGURE 9-1 Access the Compatibility tab.

4. Do one of the following:
   - To apply the setting to the currently logged-on user, select the Run This Program As An Administrator check box, and then click OK.
   - To apply the setting to all users on the computer and regardless of which shortcut is used to start the application, click Change Setting For All Users to display the Properties dialog box for the application's .exe file, select the Run This Program As An Administrator check box, and then click OK twice.

NOTE **If the Run This Program As An Administrator option is unavailable, it means that the application is blocked from always running at an elevated level, the application does not require administrator credentials to run, or you are not logged on as an administrator.**

The application will now always run using an administrator access token. Keep in mind that if you are using a standard account and prompting is disabled, the application will fail to run.

Optimizing Virtualization and Installation Prompting for Elevation

With regard to applications, two areas of User Account Control can be customized:

- Automatic installation detection and prompting
- Virtualization of write failures

In Group Policy, you can configure these features by using the Administrative Templates policies for Computer Configuration under Windows Settings\Security Settings\Local Policies\Security Options. The security settings are as follows:

- **User Account Control: Detect Application Installations And Prompt For Elevation** Determines whether Windows 7 automatically detects application installation and prompts for elevation or consent. (This setting is enabled by default in Windows 7.) If you disable this setting, users are not prompted, in which case, the users will not be able to elevate permissions by supplying administrator credentials.
- **User Account Control: Virtualize File And Registry Write Failures To Per-User Locations** Determines whether file and registry virtualization is on or off. Because this setting is enabled by default, error notifications and error logging related to virtualized files and registry values are written to the virtualized location rather than the actual location to which the application was trying to write. If you disable this setting, the application will silently fail when trying to write to protected folders or protected areas of the registry.

In a domain environment, you can use Active Directory–based Group Policy to apply the security configuration you want to a particular set of computers. You can also configure these settings on a per-computer basis by using local security policy. To do this, follow these steps:

1. Click Start, point to All Programs, Administrative Tools, and then click Local Security Policy. This starts the Local Security Policy console.
2. In the console tree, under Security Settings, expand Local Policies, and then select Security Options.
3. Double-click the setting you want to work with, make any necessary changes, and then click OK.

Installing Programs: The Essentials

Program installation is fairly straightforward. Not so straightforward are troubleshooting the many things that can go wrong and fixing problems. To solve problems that might occur, you first need to understand the installation process. In many cases, the typical installation process starts when Autorun is triggered. Autorun in turn invokes a setup program. Once the setup program starts, the installation process can begin. Part of the installation process involves checking the user's credentials to ensure that he or she has the appropriate privileges to install the program and prompting for consent if the user doesn't. As part of installing a program, you might also need to make the program available to all or only some users on a computer.

Occasionally, Windows might not be successful in detecting the required installation permissions. This can occur if the installation manifest for the program has an embedded RequestedExecutionLevel setting that has a value set as RequireAdministrator. Because the RequestedExecutionLevel setting overrides what the installer detects in Windows, the installation process fails any time you run the installer with standard user permissions. To solve this problem, back out of the failed installation by exiting, canceling the installation, or taking another appropriate action. Next, locate the executable file for the installer. Right-click this file, and then click Run As Administrator to restart the installation process with administrator privileges.

Additionally, it is important to understand that in Windows 7 and Windows Server 2008 Release 2, Application Control policies replace Software Restriction policies. Software Restriction policies control the applications that users can install and run on Windows 2000, Windows XP, and Windows Vista. Application Control policies control the applications that users can install and run on Windows 7 and Windows Server 2008 Release 2. Keep the following in mind:

- When you are editing a Group Policy object (GPO), you can create and manage Software Restriction policies by using settings for computers under Computer Configuration\Policies\Windows Settings\Security Settings\Software Restriction Policies and settings for users under User Configuration\Policies\Windows Settings\Security Settings\Software Restriction Policies. Enforcement settings control how restrictions are applied. Designated file types determine what is and what is not considered an executable program.
- When you are editing a GPO, you can create and manage Application Control policies by using settings for computers under Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies. You can now create separate rules for executable files, Windows installer files, and script files. Rules can be applied by publisher, file path, or file hash. A publisher rule gives you the most flexibility, enabling you to specify which products and versions to allow. For example, you could allow Microsoft Word 2003 or later.

Working with Autorun

When you insert an application CD or DVD into a CD or DVD drive, Windows 7 checks for a file named Autorun.inf. If present, Autorun.inf specifies the action that the operating system should take and might also define other installation parameters. Autorun.inf is a text-based file that can be opened in any standard text editor. If you were to examine the contents of one, you'd see something similar to the following code:

```
[autorun]
OPEN=SETUP.EXE AUTORUN=1
ICON=SETUP.EXE,4
SHELL=OPEN
DisplayName=Microsoft Digital Image Suite 9
ShortName=PIS
PISETUP=PIP\pisetup.exe
```

This Autorun.inf file opens a file named Setup.exe when the CD or DVD is inserted into the CD or DVD drive. Because Setup.exe is an actual program, this program is invoked. The Autorun.inf file also specifies an icon to use, the status of the shell, the program display name, the program's short name, and an additional parameter, which in this case is the location of another setup program to run.

The file that Autorun.inf specifies to open won't always be a program. Consider the following example:

```
[autorun]
OPEN=Autorun\ShelExec default.htm
```

This Autorun.inf file executes via the shell and opens a file named Default.htm in the computer's Web browser. It's important to note that even in this case, the document opened in the Web browser contains links that point to a setup program.

TIP **With an application CD or DVD in a drive, you can restart the Autorun process at any time. Simply open and then close the drive bay.**

Application Setup and Compatibility

Most applications have a setup program that uses InstallShield, Wise Install, or Microsoft Windows Installer. When you start the setup program, the installer helps track the installation process and should also make it possible to easily uninstall the program when you need to. If you are installing an older application, the setup program might use an older version of one of these installers, and this might mean the uninstall process won't completely uninstall the program.

Even if you are absolutely certain that a program has a current installer, you should consider the possibility that you will need to recover the system if something goes wrong with the installation. To help ensure that you can recover your system, check that System Restore is enabled for the drive on which you are installing the program so that System Restore can create an automatic checkpoint before installing the program.

While the installers for most current programs automatically trigger the creation of a restore point before making any changes to a computer, the installers for older programs might not. You can manually create a restore point as discussed in Chapter 17, "Handling Maintenance and Support Tasks." Then, if you run into problems, you can try to uninstall the program or use System Restore to recover the system to the state it was in prior to the program's installation.

Before installing any application, you should check to see whether it is compatible with Windows 7. To determine compatibility, you can do the following:

- Check the software packaging, which should specify whether the program is compatible. Look for the Windows 7 logo.
- Check the software developer's Web site for a list of compatible operating systems.

NOTE **As part of the compatibility check, look for updates or patches for the program. If any are available, install them after installing the program.**

Windows 7 attempts to recognize potential compatibility problems before you install applications. If it detects one, you might see a Program Compatibility Assistant dialog box after you start a program's installer. Often, this dialog box contains information about the known compatibility issues with the program, and in many cases it displays a possible solution. For example, you might be advised to install the latest service pack for the program before running the program on the computer. In some cases, the Program Compatibility Assistant might display the message "This program is blocked due to compatibility issues." Here, the program is blocked because it causes a known stability issue with Windows, and you can't create an immediate fix to work around the problem. Your only options are to click the Check For Solutions Online button or click Cancel. If you check for solutions online, the typical solution requires you to purchase an updated version of the program. If you cancel, you stop the installation process without checking for possible solutions.

If the installation continues but fails for any reason before it is fully complete (or to properly notify the operating system regarding completion), you'll also see a Program Compatibility Assistant dialog box. In this case, if the program installed correctly, click This Program Installed Correctly. If the program didn't install correctly, click Reinstall Using Recommended Settings to allow the Program Compatibility Assistant to apply one or more compatibility fixes, and then try again to run the installer.

When you start programs, Windows 7 uses the Program Compatibility Assistant to automatically make changes for known compatibility issues as well. If the Program Compatibility Assistant detects a known compatibility issue when you run an application, it notifies you about the problem and provides possible solutions for resolving the problem automatically. You can then allow the Program Compatibility

Assistant to reconfigure the application for you, or you can manually configure compatibility as discussed in the section "Configuring Program Compatibility" later in this chapter.

For legacy applications, you can also use the Compatibility Administrator (Compatadmin.exe), provided in the Windows Application Compatibility Toolkit, to create an application manifest that sets the application's run level. The Compatibility Administrator can also help identify other types of compatibility issues with legacy applications. The Windows Application Compatibility Toolkit (ACT) can be downloaded from the Microsoft Download Center (*http://download.microsoft.com*).

Making Programs Available to All or Selected Users

Usually when you install a program, the program is available to all users on a computer. This occurs because the program's shortcuts are placed in the Start Menu\Programs folder (%SystemDrive%\ProgramData\Microsoft\Windows\Start Menu\Programs) for all users so that any user who logs on to the system has access to the program. Some programs prompt you during installation to choose whether you want to install the program for all users or only for the currently logged-on user. Other programs simply install themselves only for the current user.

If setup installs a program so that it is available only to the currently logged-on user and you want other users to have access to the program, you need to take one of the following actions:

- Log on to the computer with each user account that should have access to the program, and then rerun setup to make the program available to these users. You also need to run setup again when a new user account is added to the computer and that user needs access to the program.
- For programs that don't require per-user settings to be added to the registry before running, you can in some cases make the program available to all users on a computer by adding the appropriate shortcuts to the Start Menu\Programs folder for all users. Copy or move the program shortcuts from the currently logged-on user's profile to the Start Menu\Programs folder for all users.

If you want to make a program available to all users on a computer, you can copy or move a program's shortcuts by completing the following steps:

1. Right-click the Start button, and then click Open Windows Explorer. In Windows Explorer, navigate to the currently logged on user's Programs folder. This is a hidden folder under %UserProfile%\AppData\Roaming\Microsoft\Windows\Start Menu.
2. In the Programs folder, right-click the folder for the program group or the shortcut you want to work with, and then click Copy or Cut on the shortcut menu.

3. Next, navigate to the all-users Start Menu\Programs folder. This hidden folder is under %SystemDrive%\ProgramData\Microsoft\Windows\Start Menu.
4. In the Programs folder, right-click an open space, and then click Paste. The program group or shortcut should now be available to all users of the computer.

NOTE **In the %SystemDrive%\Users folder, you'll find a folder called All Users. If you are aware of this folder, you might wonder why you didn't copy the program's shortcut for all users to a subfolder of this folder. Well, the reason is that %SystemDrive%\Users\All Users is a symbolic link to %SystemDrive%\ProgramData. A symbolic link is a pointer to where a folder actually exists. When you are working with the command prompt (Cmd.exe), you can view symbolic links and reparse points (junctions) in the current directory by entering dir /al.**

If you want to make a program available only to the currently logged-on user rather than all users on a computer, you can move a program's shortcuts by completing the following steps:

1. Right-click the Start button, and then click Open Windows Explorer. In Windows Explorer, navigate to the all-users Start Menu folder. This hidden folder is under %SystemDrive%\ProgramData\Microsoft\Windows\Start Menu.
2. In the Programs folder, right-click the folder for a program group or the program shortcut that you want to work with, and then click Cut.
3. In Windows Explorer, navigate to the currently logged-on user's Programs folder. This is a hidden folder under %UserProfile%\AppData\Roaming\Microsoft\Windows\Start Menu.
4. In the Programs folder, right-click an open space, and then click Paste. The program group or shortcut should now be available only to the currently logged-on user.

NOTE **Moving a program group or shortcut hides the fact that the program is available on the computer—it doesn't prevent other users from running the program by using the Run dialog box or Windows Explorer.**

Deploying Applications Through Group Policy

You can make applications available to users over the network through Group Policy. When you use Group Policy to deploy applications, you have two distribution options:

- The first option is to assign the application to users or computers. When an application is assigned to a computer, it is installed the next time the computer is started and is available to all users of that computer the next time users log on. When an application is assigned to a user, it is installed the next time the user logs on to the network. An assigned application can also be configured to be installed on first use. In this configuration, the application is made available through shortcuts on the user's desktop or Start menu. With install-on-first-use configured, the application is installed when the user clicks a shortcut to launch the application.

- The second option is to publish the application and make it available for installation. When you publish an application, the application can be made available through extension activation. With extension activation configured, the program is installed when a user opens any file with an extension associated with the application. For example, if a user double-clicks a file with a .doc or .docx extension, Microsoft Word could be installed automatically.

You deploy applications for computers using a Microsoft Windows Installer Package (.msi file) and policies under Computer Configuration\Policies\Software Settings\Software Installation You deploy applications for users using a Windows Installer Package (.msi file) and policies under User Configuration\Policies\Software Settings\Software Installation. The basic steps required to deploy applications through Group Policy are as follows:

1. For clients to access the Windows Installer Package, it must be located on a network share. As necessary, copy the Windows Installer Package (.msi file) to a network share that is accessible by the appropriate users.
2. In the Group Policy Management Editor, open the Group Policy object (GPO) from which you want to deploy the application. After it is deployed, the application is available to all clients to which the GPO applies. This means the application is available to computers and users in the related domain, site, or organizational unit (OU).
3. Expand Computer Configuration\Policies\Software Settings or User Configuration\Policies\Software Settings, right-click Software Installation, point to New, and then click Package.
4. Use the Open dialog box to locate the Windows Installer Package (.msi file) for the application, and then click Open. You are then given the choice to select the deployment method: Published, Assigned, or Advanced.
5. To publish or assign the program, select Published or Assigned, and then click OK. If you are configuring computer policy, the program is available the next time a computer affected by the GPO is started. If you are configuring user policy, the program is available to users in the domain, site, or OU the next time users log on. Currently logged-on users need to log off and then log on.
6. To configure additional deployment options for the program, select Advanced. You can then set additional deployment options as necessary.

Configuring Program Compatibility

If you want to install 16-bit or MS-DOS-based programs, you might need to make special considerations. Additionally, to get older programs to run, you might sometimes need to adjust compatibility options. Techniques for handling these situations are discussed in the following sections.

Special Installation Considerations for 16-Bit and MS-DOS-Based Programs

Many 16-bit and MS-DOS-based programs that don't require direct access to hardware can be installed and run on Windows 7 without any problems. However, most 16-bit and MS-DOS-based programs do not support long file names. To help ensure compatibility with these programs, Windows 7 maps long and short file names as necessary. This ensures that long file names are protected when they are modified by a 16-bit or an MS-DOS-based program. Additionally, it is important to note that some 16-bit and MS-DOS-based programs require 16-bit drivers, which are not supported on Windows 7. As a result, these programs won't run.

Most existing 16-bit and MS-DOS-based programs were originally written for Windows 3.0 or Windows 3.1. Windows 7 runs these older programs using a virtual machine that mimics the 386-enhanced mode used by Windows 3.0 and Windows 3.1. Unlike on other recent releases of Windows, on Windows 7 each 16-bit and MS-DOS-based application runs as a thread within a single virtual machine. This means that if you run multiple 16-bit and MS-DOS-based applications, they all share a common memory space. Unfortunately, if one of these applications hangs or crashes, it usually means the others will as well.

You can help prevent one 16-bit or MS-DOS-based application from causing others to hang or crash by running it in a separate memory space. To do this, follow these steps.

1. Right-click the program's shortcut icon, and then click Properties. If the program doesn't have a shortcut, create one, and then open the shortcut's Properties dialog box.
2. On the Shortcut tab, click the Advanced button. This displays the Advanced Properties dialog box.
3. Select the Run In Separate Memory Space check box.
4. Click OK twice to close all open dialog boxes and save the changes.

NOTE **Running a program in a separate memory space uses additional memory. However, you'll usually find that the program is more responsive. Another added benefit is that you are able to run multiple instances of the program—as long as all the instances are running in separate memory spaces.**

TIP **The Windows 7 command prompt (Cmd.exe) is a 32-bit command prompt. If you want to invoke a 16-bit MS-DOS command prompt, you can use Command.com. Type command in the Run dialog box.**

Forcing Program Compatibility

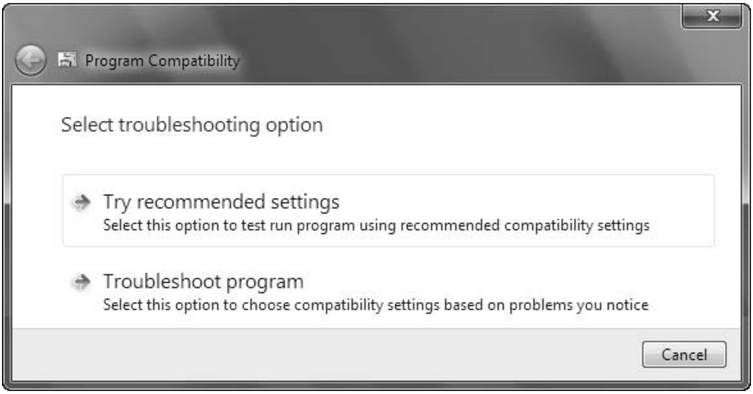
Some programs won't install or run on Windows 7 even if they work on previous versions of the Windows operating system. If you try to install a program that has known compatibility problems, Windows 7 should display a warning prompt telling you about the compatibility issue. In most cases, you should not continue installing or running a program with known compatibility problems, especially if the program is a system utility such as an antivirus program or a disk partitioning program, because running an incompatible system utility can cause serious problems. Running other types of incompatible programs can also cause problems, especially if they write to system locations on disk.

That said, if a program will not install or run on Windows 7, you might be able to run the program by adjusting its compatibility settings. Windows 7 provides two mechanisms for managing compatibility settings. You can use the Program Compatibility wizard, or you can edit the program's compatibility settings directly by using the program's Properties dialog box. Both techniques work the same way. However, the Program Compatibility wizard is the only way you can change compatibility settings for programs that are on shared network drives, CD or DVD drives, or other types of removable media drives. As a result, you can sometimes use the Program Compatibility wizard to install and run programs that would not otherwise install and run.

Using the Program Compatibility Wizard

You can only configure compatibility settings for programs you've installed. You can't configure compatibility settings for programs included with the operating system. To try to automatically detect compatibility issues using the Program Compatibility wizard, follow these steps.

1. Locate the program shortcut by navigating the menus under Start, All Programs. Right-click the program shortcut, and then click Troubleshoot Compatibility. This starts the Program Compatibility wizard, shown in Figure 9-2.


Program Compatibility

Select troubleshooting option

Select this option to test run program using recommended compatibility settings

Select this option to choose compatibility settings based on problems you notice

FIGURE 9-2 Troubleshoot program compatibility issues.

2. The wizard automatically tries to detect compatibility issues. To try to run the program you are troubleshooting with the recommended fixes, click Try Recommended Settings. Next, review the settings that will be applied, and then click Start The Program.
3. After running the program, click Next, and then do one of the following:
   - Click Yes, Save These Settings For This Program if the compatibility settings resolved the problem and you want to keep the settings.
   - Click No, Try Again Using Different Settings if the compatibility settings didn't resolve the problem and you want to repeat this process from the beginning.
   - Click No, Report The Problem To Microsoft And Check Online For A Solution if the compatibility settings didn't resolve the problem and you'd like to check for an online solution.
   - Click Cancel if you want to discard the compatibility settings and exit the wizard.

To perform advanced troubleshooting and use the Program Compatibility wizard to specify the compatibility settings to use, follow these steps:

1. Locate the program shortcut by navigating the menus under Start, All Programs. Right-click the program shortcut, and then click Troubleshoot Compatibility. This starts the Program Compatibility wizard.
2. Click Troubleshoot Program. On the What Problems Do You Notice? page, you can specify information about problems you've seen. The selections you make determine the wizard pages you see when you click Next. They include the following:
   - **The Program Worked On Earlier Versions Of Windows But Won't Install Or Run Now** If you select this option, you are prompted on one of the subsequent wizard pages to specify which version. Because your

choice sets the compatibility mode, choose the operating system for which the program was designed. When running the program, Windows 7 simulates the environment for the specified operating system.

- **The Program Opens But Doesn't Display Correctly** If you are trying to run a game, an educational program, or any other program that requires specific display settings, such as a program designed for Windows 98, you can select this option and then choose the type of display problem you are seeing. Your selections restrict the video display: when you use 256 colors, 640 × 480 screen resolution, or both, Windows restricts the video display. This can help with programs that have problems running at higher screen resolutions and greater color depths. Your selections can also disable themes, desktop compositing (which prevents special visual effects on the desktop), and display scaling of high dots-per-inch (DPI) settings.
- **The Program Requires Additional Permissions** If you choose this option, the program will be configured to run with administrator privileges.
- **I Don't See My Problem Listed** If you choose this option, the wizard displays optional pages for operating system and display issue selection. The wizard also sets the program to run as an administrator. Ultimately, choosing this option has the same effect as if you had selected all three of the previous options.

3. Review the compatibility settings that will be applied. If you don't want to apply these settings, click Cancel and repeat this procedure to select different options. If you want to apply these settings, click Start The Program, and the wizard runs the program with the compatibility settings you specified.
4. After running the program, click Next to continue. When you continue, you are prompted to confirm whether the changes fixed the problem. Do one of the following:
   - If the compatibility settings resolved the problem and you want to keep the settings, click Yes, Save These Settings For This Program.
   - If the compatibility settings didn't resolve the problem and you want to repeat this process from the beginning, click No, Try Again Using Different Settings.
   - If the compatibility settings didn't resolve the problem and you'd like to check for an online solution, click No, Report The Problem To Microsoft And Check Online For A Solution.
   - If you want to discard the compatibility settings and exit the wizard, click Cancel.

NOTE **If you've configured alternate display settings for an application, the application will run in the alternate display mode whenever you start it. To restore the original display settings, simply exit the program.**

Setting Compatibility Options Directly

If a program you have already installed won't run correctly, you might want to edit the compatibility settings directly rather than through the wizard. To do this, follow these steps.

1. Right-click the program's shortcut icon, and then click Properties.
2. In the Properties dialog box, click the Compatibility tab. Any option you select is applied to the currently logged-on user for the application shortcut. To apply the setting to all users on the computer and regardless of which shortcut is used to start the application, click Change Setting For All Users to display the Properties dialog box for the application's .exe file, and then select the compatibility settings that you want to use for all users who log on to the computer.

   NOTE **Programs that are part of the Windows 7 operating system cannot be run in Compatibility mode. The options on the Compatibility tab are not available for built-in programs.**

3. Select the Run This Program In Compatibility Mode For check box, and then use the selection menu to choose the operating system for which the program was designed.
4. If necessary, use the options in the Settings panel to restrict the video display settings for the program. Select 256 colors, 640 × 480 screen resolution, or both, as required.
5. If necessary, you can also disable visual themes, desktop compositing, and display scaling of high DPI settings.
6. Click OK. Double-click the shortcut to run the program and test the compatibility settings. If you still have problems running the program, you might need to modify the compatibility settings again.

Managing Installed and Running Programs

Windows 7 provides several management tools for working with programs. These tools include:

- **Task Manager** Provides options for viewing and managing running programs as well as options for viewing resource usage and performance
- **Programs** Provides tasks for viewing installed programs, adding and removing programs, viewing installed updates, and more
- **Default Programs** Helps you track and configure global default programs for the computer, personal default programs for individual users, AutoPlay settings for multimedia, and file associations for programs

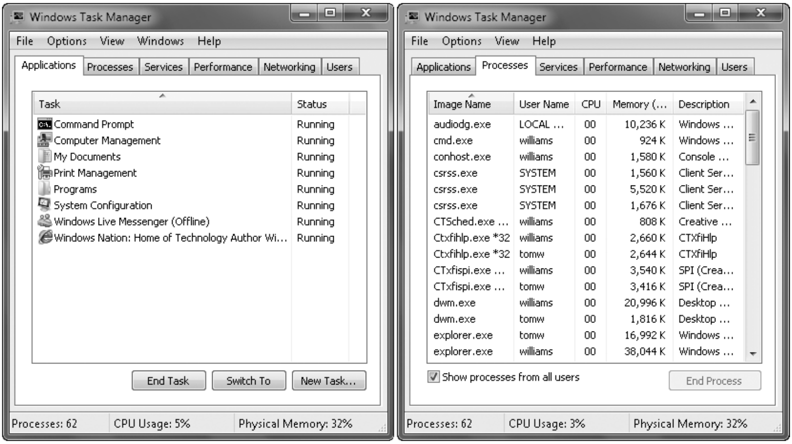
- **Windows Features** Helps you view and manage the Windows components installed on a computer
- **Assoc** Helps you view and manage file type associations
- **Ftype** Helps you view and manage file type definitions

These tools and related configuration options are discussed in the sections that follow.

Managing Currently Running Programs

In Windows 7, you can view and work with a computer's currently running programs and processes by using Task Manager. You can open Task Manager by pressing Ctrl+Alt+Delete and then selecting Start Task Manager. As Figure 9-3 shows, Task Manager has two tabs for working with running programs:

- **Applications** Lists applications that are currently running in the foreground by name and status (such as Running or Not Responding). To exit a program, which might be necessary when it is not responding, click the program in the Task list, and then click End Task.
- **Processes** Lists all background and foreground applications running on the computer by image name, user name, and resource usage. To stop a process, click the process, and then click End Process.



Task	Status
Command Prompt	Running
Computer Management	Running
My Documents	Running
Print Management	Running
Programs	Running
System Configuration	Running
Windows Live Messenger (Offline)	Running
Windows Nation: Home of Technology Author Wi...	Running

Processes: 62 CPU Usage: 5% Physical Memory: 32%

Image Name	User Name	CPU	Memory (...	Description
audiodg.exe	LOCAL ...	00	10,236 K	Windows ...
cmd.exe	williams	00	924 K	Windows ...
conhost.exe	williams	00	1,580 K	Console ...
csrss.exe	SYSTEM	00	1,560 K	Client Ser...
csrss.exe	SYSTEM	00	5,520 K	Client Ser...
csrss.exe	SYSTEM	00	1,676 K	Client Ser...
CTSched.exe ...	williams	00	808 K	Creative ...
Ctxfihlp.exe *32	williams	00	2,660 K	CTXfiHlp
Ctxfihlp.exe *32	tomw	00	2,644 K	CTXfiHlp
CTxfispi.exe ...	williams	00	3,540 K	SPI (Crea...
CTxfispi.exe ...	tomw	00	3,416 K	SPI (Crea...
dwm.exe	williams	00	20,996 K	Desktop ...
dwm.exe	tomw	00	1,816 K	Desktop ...
explorer.exe	tomw	00	16,992 K	Windows ...
explorer.exe	williams	00	38,044 K	Windows ...

☑ Show processes from all users

Processes: 62 CPU Usage: 3% Physical Memory: 32%

FIGURE 9-3 Use Task Manager to work with running applications and processes.

While the details for process count, CPU usage, and physical memory usage are for the computer as a whole, the processes are only listed for the currently logged-on user and the operating system by default. To see running processes for all users, you must click Show Processes From All Users.

TIP On the Processes tab, you can manage processes in additional ways by right-clicking a process and selecting from an extended list of options. The options include Open File Location, which opens the folder containing the executable file for the process in Windows Explorer; End Process Tree, which stops the process and all dependent processes; Create Dump File, which creates a memory dump file for the selected process; and Properties, which opens the Properties dialog box for the executable file.

Managing, Repairing, and Uninstalling Programs

Windows 7 considers any program you've installed on a computer or made available for a network installation to be an installed program. In Windows XP and earlier versions, you use the Add Or Remove Programs utility to install and manage applications. In Windows 7, you use the setup program that comes with the application to install applications, and you use the Installed Programs page in Control Panel to manage applications.

You can use the Installed Programs page to view, add, remove, or repair installed programs by following these steps:

1. Click Start, and then click Control Panel. In Control Panel, click Programs.
2. Click Programs And Features. You should see a list of installed programs.
3. In the Name list, right-click the program you want to work with, and then click one of the following commands:
   - **Uninstall** to uninstall the program
   - **Change** to modify the program's configuration
   - **Repair** to repair the program's installation

When you are uninstalling programs, keep the following in mind:

- Windows warns you if you try to uninstall a program while other users are logged on. Generally, you should be sure that other users are logged off before uninstalling programs. Otherwise, you might cause other users to lose data or experience other problems.
- Windows will allow you to remove only those programs that were installed with a Windows-compatible setup program. Although most applications have a setup program that uses InstallShield, Wise Install, or Microsoft Windows Installer, older programs might have a separate uninstall utility. Some older programs work by copying their data files to a program folder. In this case, you uninstall the program by deleting the related folder.
- Many uninstall programs leave behind data either inadvertently or by design. As a result, you often find folders for these applications within the Program Files folder. You could delete these folders, but they might contain important data files or custom user settings that could be used again if you reinstall the program.

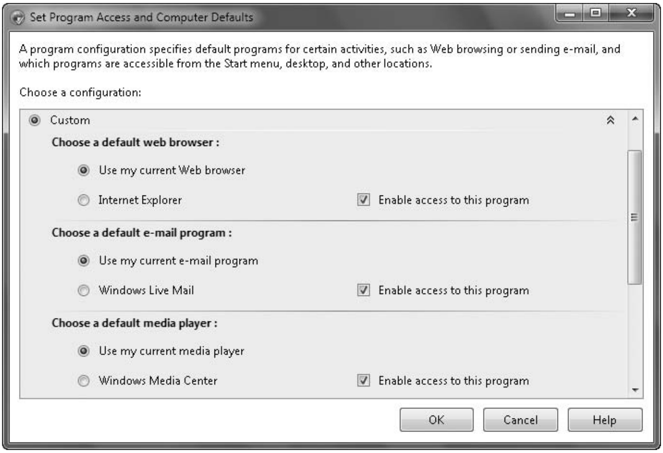
- Sometimes, the uninstall process fails. Often, you can resolve any problem simply by rerunning the uninstaller for the program. Occasionally, you might need to clean up after the uninstall process. This might require removing program files and deleting remnants of the program in the Windows registry. A program called the Windows Installer Cleanup utility can help you clean up the registry. For more information on the utility and to download the software, see the article on the Microsoft support Website at *http://support.microsoft.com/kb/290301*).

Designating Default Programs

Default programs determine which programs are used with which types of files and how Windows handles files on CDs, DVDs, and portable devices. You configure default programs based on the types of files those programs support, either globally for all users of a computer or only for the current user. Individual user defaults override global defaults. For example, you could select Windows Media Player as the global default for all types of files it supports, and then all users of the computer would use Windows Media Player to play the sound, audio, and video files it supports. If a specific user wanted to use Apple iTunes instead as the default player for sound and audio files, you could configure iTunes to be that user's default player for the types of media files it supports.

You can configure global default programs for all the users of a computer by following these steps:

1. Click Start, and then click Control Panel. In Control Panel, click Programs.
2. Click Default Programs, and then click Set Program Access And Computer Defaults. You'll see the dialog box shown in Figure 9-4.



Set Program Access and Computer Defaults

A program configuration specifies default programs for certain activities, such as Web browsing or sending e-mail, and which programs are accessible from the Start menu, desktop, and other locations.

Choose a configuration:

● Custom

Choose a default web browser :

● Use my current Web browser

○ Internet Explorer ☑ Enable access to this program

Choose a default e-mail program :

● Use my current e-mail program

○ Windows Live Mail ☑ Enable access to this program

Choose a default media player :

● Use my current media player

○ Windows Media Center ☑ Enable access to this program

FIGURE 9-4 Choose a global default configuration.

3. Choose a configuration from one of the following options:
   - **Microsoft Windows** Sets the currently installed Windows programs as the default programs for browsing the Web, sending e-mail, playing media files, and so on.
   - **Non-Microsoft** Sets the currently installed programs as the default programs for browsing the Web, sending e-mail, playing media files, and so on.
   - **Custom** Enables you to choose programs as the defaults for browsing the Web, sending e-mail, playing media files, and so on.
4. Click OK to save the settings.

To override global defaults, you can set default programs for individual users. You can configure default programs for the current user by following these steps:

1. Click Start, and then click Control Panel. In Control Panel, click Programs.
2. Click Default Programs, and then click Set Your Default Programs.
3. Select a program you want to work with in the Programs list.
4. If you want the program to be the default for all the file types and protocols it supports, click Set This Program As Default.
5. If you want the program to be the default for specific file types and protocols, click Choose Defaults For This Program. Select the file extensions for which the program should be the default, and then click Save.

Managing the Command Path

Windows uses the command path to locate executables. You can view the current command path for executables by using the PATH command. In a command shell, type **path** on a line by itself, and then press Enter. In a Windows PowerShell console, type **$env:path** on a line by itself, and then press Enter. In the output, observe that Windows uses a semicolon (;) to separate individual paths, marking where one file path ends and another begins.

The command path is set during logon by using system and user environment variables. The path defined in the PATH system variable sets the base path. The path defined in the PATH user variable adds to the base path by using the following syntax:

```
%PATH%;AdditionalPaths
```

Here, %PATH% tells Windows to insert the current system paths, and *AdditionalPaths* designates the additional user-specific paths to use.

> ***CAUTION*** **An improperly set path can cause severe problems. You should always test any command path change before using it in a live environment. The command path is set during logon. Therefore, you must log off and then log on again to see the effects of the revised path.**

Don't forget about the search order that Windows uses. Paths are searched in order, with the last path in the PATH user variable being the last one searched. This can sometimes slow the execution of your programs and scripts. To help Windows find your programs and scripts faster, you should consider placing a required path earlier in the search order.

Be careful when setting the command path. It is easy to overwrite all path information accidentally. For example, if you don't specify %PATH% when setting the user path, you will delete all other path information. One way to ensure that you can easily re-create the command path is to keep a copy of the command path in a file.

- When you are working with the command prompt, you can write the current command path to a file by entering **path > orig_path.txt**. Keep in mind that if you are using a standard command prompt rather than an administrator command prompt, you won't be able to write to secure system locations. In this case, you can write to a subdirectory to which you have access or to your personal profile. To write the command path to the command-shell window, type **path**.
- When you are working with the PowerShell console, you can write the current command path to a file by entering **$env:path > orig_path.txt**. If you are using a standard console rather than an administrator console, you won't be able to write to secure system locations. In this case, you can write to a subdirectory to which you have access or to your personal profile. To write the command path to the PowerShell window, type **$env:path**.

At the command prompt or in the PowerShell window, you can modify the command path by using the Setx.exe utility. You also can edit the command path by completing the following steps:

1. In Control Panel, click System And Security, and then click System.
2. In the System console, click Change Settings, or click Advanced System Settings in the left pane.
3. On the Advanced tab in the System Properties dialog box, click the Environment Variables button.
4. Select the PATH variable in the System Variables list. Under System Variables, click Edit.
5. By default, the path value is selected. Without pressing any other key, press the Right Arrow key. This should remove the selection highlight and place the insertion point at the end of the variable value.
6. Type a semicolon, and then enter a path to insert. Repeat as necessary, and then click OK three times.

In Group Policy, you can use a preference item to modify the command path. Follow these steps:

1. Open a Group Policy object (GPO) for editing in the Group Policy Management Editor. To configure preferences for computers, expand Computer

Configuration\Preferences\Windows Settings, and then select Environment. To configure preferences for users, expand User Configuration\Preferences\Windows Settings, and then select Environment.

2. Right-click the Environment node, point to New, and then click Environment Variable. This opens the New Environment Properties dialog box.
3. In the Action list, select Update to update the path variable, or select Replace to delete and then re-create the path variable. Next, select User Variable to work with user variables.
4. In the Name field, type **Path**. In the Value field, type the variable value. Typically, you'll enter **%PATH%;** followed by the paths you want to add, using a semicolon to separate each path. If the affected computers have existing PATH user variable definitions, you must provide the related paths to ensure that these paths are retained.
5. Use the options on the Common tab to control how the preference is applied. In most cases, you'll want to create the PATH variable only once (rather than have Group Policy re-create the variable each time policy is refreshed). If so, select Apply Once And Do Not Reapply.
6. Click OK. The next time policy is refreshed, the preference item will be applied as appropriate for the GPO in which you defined the preference item.

CAUTION **Incorrectly setting the path can cause serious problems. Before deploying an updated path to multiple computers, you should test the configuration. One way to do this is to create a GPO in Active Directory that applies only to an isolated test computer. Next, create a preference item for this GPO, and then wait for a policy to refresh or apply policy using GPUpdate. If you are logged on to the computer, you need to log off and then log back on before you can confirm the results.**

Managing File Extensions and File Associations

File extensions and file associations also are important for determining how programs run. The types of files that Windows considers to be executables are determined by the file extensions for executables. File extensions allow users to execute a command by using just the command name. File associations are what allow users to double-click a file and open the file automatically in a related application. Two types of file extensions are used:

- **File extensions for executables** Executable files are defined with the %PATHEXT% environment variable and can be set using the Environment Variables dialog box or with Group Policy preference items in much the same way as the PATH variable. You can view the current settings by typing **set pathext** at the command line or by typing **$env:pathext** at a PowerShell prompt. The default setting is PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC. With this setting, the command line knows which files are executable and which files are not, so you don't have to specify the file extension at the command line.

- **File extensions for applications** File extensions for applications are referred to as file associations. File associations are what enable you to pass arguments to executables and to open documents, worksheets, or other application files by double-clicking their file icons. Each known extension on a system has a file association that you can view at a command prompt by typing **assoc** followed by the extension, such as **assoc .doc** or **assoc .docx**. Each file association in turn specifies the file type for the file extension. This can be viewed at a command prompt by typing **ftype** followed by the file association, such as **ftype Word.Document.8** or **ftype Word.Document.12**.

NOTE **Assoc and Ftype are internal commands for the command shell (Cmd.exe). To use the Assoc command in PowerShell, enter cmd /c assoc followed by the extension, such as cmd /c assoc .doc. To use the Ftype command in PowerShell, enter cmd /c ftype followed by the file association, such as cmd /c ftype Word.Document.8.**

With executables, the order of file extensions in the %PATHEXT% variable sets the search order used by the command line on a per-directory basis. Thus, if a particular directory in the command path has multiple executables that match the command name provided, a .com file would be executed before an .exe file and so on.

Every known file extension on a system has a corresponding file association and file type—even extensions for executables. In some cases, the file type is the extension text without the period followed by the keyword file, such as cmdfile, exefile, or batfile, and the file association specifies that the first parameter passed is the command name and that other parameters should be passed on to the application. For example, if you type **assoc .exe** to see the file associations for .exe executables, you then type **ftype exefile**. You'll see the file association is set to the following:

```
exefile="%1" %*
```

Thus, when you run an .exe file, Windows knows the first value is the command that you want to run and anything else provided is a parameter to pass along.

File associations and types are maintained in the Windows registry and can be set using the Assoc and Ftype commands, respectively. To create the file association at the command line, type **assoc** followed by the extension setting, such as **assoc .pl=perlfile**. To create the file type at the command line, set the file-type mapping, including how to use parameters supplied with the command name, such as **ftype perlfile=C:\Perl\Bin\Perl.exe "%1" %***.

You also can associate a file type or protocol with a specific program by completing the following steps:

1. Click Start, and then click Control Panel. In Control Panel, click Programs.
2. Click Default Programs, and then click Associate A File Type Or Protocol With A Program.

3. On the Set Associations page, current file associations are listed by file extension and the current default for that extension. To change the file association for an extension, click the file extension, and then click Change Program.
4. Do one of the following:
   - The Recommended Programs list shows programs that are registered in the operating system as supporting files with the selected extension. Click a recommended program to set it as the default for the selected extension, and then click OK.
   - The Other Programs list shows programs that might also support the selected extension. Click a program to set it as the default for the selected extension, and then click OK. Alternatively, click Browse to locate another program to use as the default.

In Group Policy, you can use a preference item to create new file types and file associations. To create a preference item for a new file type, follow these steps:

1. Open a Group Policy object (GPO) for editing in the Group Policy Management Editor. Expand Computer Configuration\Preferences\Control Panel Settings, and then select Folder Options.
2. Right-click the Folder Options node, point to New, and then click File Type. This opens the New File Type Properties dialog box.
3. In the Action list, select Create, Update, Replace, or Delete.
4. In the File Name Extension field, type the extension of the file type without the period, such as **pl**.
5. In the Associated Class list, select a registered class to associate with the file type.
6. Use the options on the Common tab to control how the preference is applied. In most cases, you'll want to create the new variable only once. If so, select Apply Once And Do Not Reapply.
7. Click OK. The next time policy is refreshed, the preference item will be applied as appropriate for the GPO in which you defined the preference item.

To create a preference item for a new file association, follow these steps:

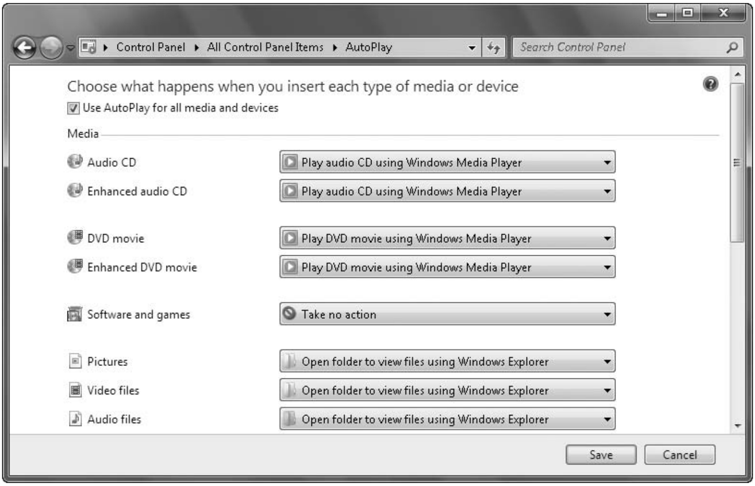
1. Open a Group Policy object (GPO) for editing in the Group Policy Management Editor. Expand User Configuration\Preferences\Control Panel Settings, and then select Folder Options.
2. Right-click the Folder Options node, point to New, and then click Open With. This opens the New Open With Properties dialog box.
3. In the Action list, select Create, Update, Replace, or Delete.
4. In the File Name Extension field, type the extension of the file type without the period, such as **pl**.

5. Click the Browse (...) button to the right of the Associated Program field, and then use the Open dialog box to select the program to associate with the file type.
6. Optionally, select Set As Default to make the associated program the default for files with the previously specified file extension.
7. Use the options on the Common tab to control how the preference is applied. In most cases, you'll want to create the new variable only once. If so, select Apply Once And Do Not Reapply.
8. Click OK. The next time policy is refreshed, the preference item will be applied as appropriate for the GPO in which you defined the preference item.

Configuring AutoPlay Options

In Windows 7, AutoPlay options determine how Windows handles files on CDs, DVDs, and portable devices. You can configure separate AutoPlay options for each type of CD, DVD, and media your computer can handle by following these steps:

1. Click Start, and then click Control Panel. In Control Panel, click Programs.
2. Click Default Programs, and then click Change AutoPlay Settings. This displays the AutoPlay page in Control Panel.
3. As shown in Figure 9-5, use the media selection list to set the default AutoPlay option for each media type.



Choose what happens when you insert each type of media or device

☑ Use AutoPlay for all media and devices

Media

Audio CD	Play audio CD using Windows Media Player
Enhanced audio CD	Play audio CD using Windows Media Player
DVD movie	Play DVD movie using Windows Media Player
Enhanced DVD movie	Play DVD movie using Windows Media Player
Software and games	Take no action
Pictures	Open folder to view files using Windows Explorer
Video files	Open folder to view files using Windows Explorer
Audio files	Open folder to view files using Windows Explorer

FIGURE 9-5 Set AutoPlay options for CDs, DVDs, and portable devices.

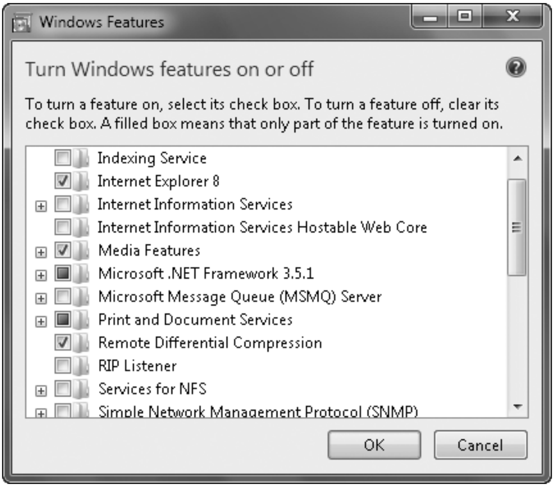
4. Click Save to save your settings.

Adding and Removing Windows Features

In Windows XP and earlier versions of Windows, you use the Add/Remove Windows Components option of the Add Or Remove Programs utility to add or remove operating system components. In Windows Vista and Windows 7, operating system components are considered Windows features that can be turned on or off rather than added or removed.

You can turn on or off Windows features by following these steps:

1. Click Start, and then click Control Panel. In Control Panel, click Programs.
2. Under Programs And Features, click Turn Windows Features On Or Off. This displays the Windows Features dialog box.
3. As shown in Figure 9-6, select the check boxes for features to turn them on, or clear the check boxes for features to turn them off.



Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ☐ Indexing Service
- ☑ Internet Explorer 8
- ⊞ ☐ Internet Information Services
- ☐ Internet Information Services Hostable Web Core
- ⊞ ☑ Media Features
- ⊞ ■ Microsoft .NET Framework 3.5.1
- ⊞ ☐ Microsoft Message Queue (MSMQ) Server
- ⊞ ■ Print and Document Services
- ☑ Remote Differential Compression
- ☐ RIP Listener
- ⊞ ☐ Services for NFS
- ⊞ ☐ Simple Network Management Protocol (SNMP)

FIGURE 9-6 Add or remove operating system components.

4. Click OK, and Windows 7 reconfigures components for any changes you made.

Index

About the Author

WILLIAM R. STANEK (*www.williamstanek.com/*) has more than 20 years of hands-on experience with advanced computer programming and software development. He is a leading technology expert, an award-winning author, and a pretty-darn-good instructional trainer. Over the years, his practical advice has helped millions of programmers, developers, and network engineers all over the world. He has written more than 100 books. His recent books include *Active Directory Administrator's Pocket Consultant*, *Windows Group Policy Administrator's Pocket Consultant*, *Windows PowerShell 2.0 Administrator's Pocket Consultant*, and *Windows Server 2008 Inside Out* (all from Microsoft Press).

William has been involved in the commercial Internet community since 1991. His core business and technology experience comes from more than 11 years of military service. He has substantial experience in developing server technology, encryption, and Internet solutions. He has written many technical white papers and training courses on a wide variety of topics. He frequently serves as a subject matter expert and consultant.

William has a BS in computer science, magna cum laude, and an MS with distinction in information systems. He is proud to have served in the Persian Gulf War as a combat crewmember on an electronic warfare aircraft. He flew on numerous combat missions into Iraq and was awarded nine medals for his wartime service, including one of the United States of America's highest flying honors, the Air Force Distinguished Flying Cross. Currently, he resides in the Pacific Northwest with his wife and children.

Follow William on Twitter at WilliamStanek.