chapter 16

NTFS, Users, and Groups

"Only the insecure strive for security."

—Wayne Dyer

In this chapter, you will learn how to

- Create and administer Windows users and groups
- Define and use NTFS permissions for authorization
- Share a Windows computer securely
- Secure PCs with User Account Control

If you asked me what keeps Windows the number one operating system in the world, I'd say "Windows is the easiest operating system for securing resources, individual computers, and entire networks." Windows gets it right when it comes to protection. Using a combination of user accounts and groups that tie into the NTFS file system, Windows provides incredibly powerful file and folder protection. This user/group/NTFS combo scales from a single computer up to a network of computers spanning the world. Windows doesn't just stop at files and folders, either.

To understand security in Windows, you need to see it from Windows' point of view. In Windows, sharing files between users on a single machine and sharing files with users over a network are the same. When learning about users, groups, and NTFS permissions, however, it's helpful to think about a single PC. To that end, this chapter focuses on Windows security from the point of view of a single, or *standalone*, machine. I may dip into networks and domains from time to time, especially when the only differences are cosmetic, but Chapter 29 will revisit these topics in more detail and show you how the same tools scale up to help you protect a computer in a networked environment.

Authentication with Users and Groups

We've discussed the concept of users and groups in earlier chapters, but have you ever considered what user accounts and passwords actually do? To better understand their roles, you need to know two terms: authentication and authorization. **Authentication** is the process by which you determine a person at your computer is who he says he is and then grant him entry into the computer. In Windows, authentication is handled by a password-protected user account. Once a user is authenticated, he needs **authorization**, which controls what an authenticated user can and cannot do on a system. Authorization for Windows' files and folders is controlled by the NTFS file system, which assigns permissions to users, groups, or both.

Microsoft's answer to the authentication/authorization process is amazing. Inside every Windows computer is a database of user accounts—an encrypted list of user names with their associated password—who are allowed access to the system. Each of these individual records is called a **local user account**. If you don't have a local user account created on a particular system, you won't be able to log on to that computer (see Figure 16.1).

Tech Tip

Principle of Least Privilege

A good security practice to determine what type of user account to give to a specific person is the principle of least privilege. *In essence, you want to give users just enough—but no more—permissions to accomplish their tasks. Giving more than needed begs for problems or accidents and should be avoided.*

• Figure 16.1 Windows logon screen

Every local user account needs a password (even if it's blank) and needs to belong to a group. Configuring these attributes requires tools in Windows for creating and managing users and groups. The tools used in Windows XP, however, are not the same as the tools used in Windows Vista or Windows 7. Each version of Windows includes one or two ways to deal with users and groups. Home editions of Windows (such as Windows XP Home Edition, Windows Vista Home Basic and Home Premium, and Windows 7 Home Premium) include a basic tool, while the professional editions of Windows (Windows XP Professional; Windows Vista Business, Ultimate, and Enterprise; and Windows 7 Professional, Ultimate, and Enterprise) include an extra, more advanced utility. That's a lot to learn about, and I'll explain all of these tools later in the chapter. First, I want to explain passwords and groups, which are common to users across all versions of Windows.

To create and manage users, you must have administrator privileges.

Passwords

Passwords are the ultimate key to protecting your computer. If someone learns your user name and password, they can log on to your computer. Even if the user account has only limited permissions—perhaps it can only read files, not edit them—you still have a security breach. Remember: for a hacker, just getting into the computer is half the battle.

Protect your passwords. Never give out passwords over the phone. If a user forgets a password, the network administrator should reset it to a complex combination of letters and numbers. The user should then change the password to something he or she wants, according to the parameters set by the administrator.

Make your users choose good passwords. I once attended a security seminar, and the speaker had everyone stand up. She then began to ask questions about our passwords—if we responded yes to the question, we were to sit down. She began to ask questions such as

"Do you use the name of your spouse as a password?" and

"Do you use your pet's name?"

By the time she had asked about 15 questions, only 6 people out of some 300 were still standing. The reality is that most of us choose passwords that are amazingly easy to hack. Make sure you use a **strong password**: at least eight characters in length, including letters, numbers, and punctuation symbols.

Using non-alphanumeric characters makes any password much more difficult to crack, for two reasons. First, adding non-alphanumeric characters forces the hacker to consider many more possible characters than just letters and numbers. Second, most password crackers use a combination of common words and numbers to hack passwords.

Because non-alphanumeric characters don't fit into common words or numbers, a character such as an exclamation point defeats these common-word hacks. Not all systems allow you to use characters such as @, $, %, or \, however, so you need to experiment.

CompTIA also recommends that you should have users change passwords at regular intervals. Although this concept sounds good on paper, it is a hard policy to maintain in the real world. For starters, users tend to forget passwords when they change a lot. This can lead to an even bigger security problem because users start writing passwords down.

If your organization forces you to change passwords often, one way to remember the password is to use a numbering system. I worked at a company that required me to change my password at the beginning of each month, so I did something very simple. I took a root password—let's say it was "m3y3rs5"—and simply added a number to the end representing the current month. So when June rolled around, for example, I would change my password to "m3y3rs56." It worked pretty well!

Every secure organization sets up various security policies and procedures to ensure that security is maintained. Windows has various mechanisms to implement such things as requiring a strong password, for example. Chapter 29 goes into detail about setting up Local Policies and Group Policy.

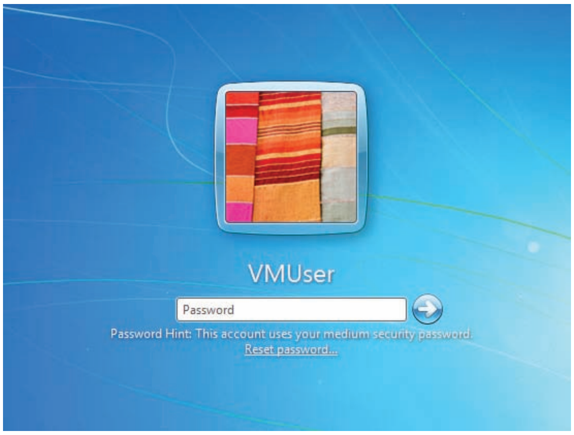
Windows enables logged-on users to create a **password reset disk** they can use if they forget a password. This is very important to have. If you lose your password and an administrator resets it, you might not have access to all of the files you had access to before, especially if they were encrypted. When you reset a password with a password reset disk, you can log on with the new password and still have access to previously encrypted files.

Best of all, password reset disks enable users to fix their own passwords. Encourage your users to create this disk; they only have this power if they create a password reset disk *before* they forget the password! Windows Vista and Windows 7 have an obvious option in the Tasks list to *Create a password reset disk*. You need a USB flash drive to create the disk. If by some chance you still have a floppy drive, you can use a floppy disk—which is where the term "disk" in password reset disk came from.

In addition to supporting password reset disks, Windows 7 enables you to create a password hint for your accounts. This clue appears after your first logon attempt fails (see Figure 16.2).

Blank passwords or passwords that are easily visible on a sticky note provide no security. Always insist on non-blank passwords, and do not let anyone leave a password sitting out in the open.

Be aware that if your computer is a member of a domain, you cannot use password reset disks or password hints to recover your password. In



Password Hint: This account uses your medium security password.

• **Figure 16.2** Password hint on the Windows 7 logon screen those cases, the network administrator has to reset your password on the domain controller.

Groups

A **group** is a collection of user accounts that can define the capabilities of its members. A single account can be a member of multiple groups. Groups are an efficient way of managing multiple users, especially when you are dealing with a whole network of accounts.

Groups make Windows administration much easier in two ways. First, you can assign a certain level of access for a file or folder to a group instead of to just a single user account. You can make a group called Accounting, for example, and put all the accounting user accounts in that group. If a person quits, you don't need to worry about assigning all of the proper access levels when you create a new account for his or her replacement. After you make an account for the new person, just add his account to the appropriate access group! Second, Windows provides numerous built-in groups with various access levels already predetermined. As you might imagine, there are differences among the versions of Windows, as described next.

Groups in Windows XP

Windows XP Professional provides seven built-in groups: Administrators, Power Users, Users, Backup Operators, Replicator, Everyone, and Guests. These built-in groups have a number of preset capabilities. You cannot delete these groups. Here's what you need to know about the five most important groups:

- **Administrators** Any account that is a member of the **Administrators group** has complete administrator privileges. Administrator privileges grant complete control over a machine. It is common for the primary user of a Windows system to have her account in the Administrators group.
- **Power Users** Members of the **Power Users group** are almost as powerful as Administrators, but they cannot install new devices or access other users' files or folders unless the files or folders specifically provide them access.
- **Users** Members of the **Users group** cannot edit the Registry or access critical system files. They can create groups but can manage only those they create.
- **Everyone** This group applies to any user who can log on to the system. You cannot edit this group.
- **Guests** The **Guests group** enables someone who does not have an account on the system to log on by using a guest account. You might use this feature at a party, for example, to provide casual Internet access to guests, or at a library terminal. Most often, the guest account remains disabled.

If you're running Windows XP Professional on a Windows domain, all of the groups listed previously are included, plus other specialized groups like HelpServicesGroup and Remote Desktop Users.

Windows XP Home Edition uses groups like its big, professional brother, but never shows the user. In fact, Home Edition only enables you to use three groups: Administrators, Users, and Guests. You'll understand more when I explain how to manage users in Windows XP, but for now, know that groups are severely limited in the Home Edition of Windows XP.

Groups in Windows Vista and Windows 7

The professional editions of Windows Vista (Business, Ultimate, and Enterprise) and Windows 7 (Professional, Ultimate, and Enterprise) offer the same groups found in Windows XP Professional and throw in a lot more. Some of the default groups, such as Distributed COM Users, target specific roles in certain industries and mean little for the average user or tech. Other specific groups enable people to check on the performance and reliability of a computer without gaining access to any of the documents on the computer. These groups include Event Log Readers, Performance Log Users, and Performance Monitor Users. These groups provide excellent levels of access for technicians to help keep busy Vista/7 machines healthy.

Windows Vista Enterprise and Windows 7 Enterprise users will almost always log on to a domain.

Like Windows XP, the home editions of Windows Vista and 7 (Home Basic and Home Premium) offer only three groups: Administrators, Users, and Guests. Administrators and Guests function as they do in all of the other versions of Windows. Members of the Users group, on the other hand, are called **standard users** and differ significantly from the limited users of Windows XP infamy. Standard users are prevented from harming the computer or uninstalling applications but can run most applications. Technicians don't have to run over to standard user accounts to enable access to common tasks such as printing or doing e-mail.

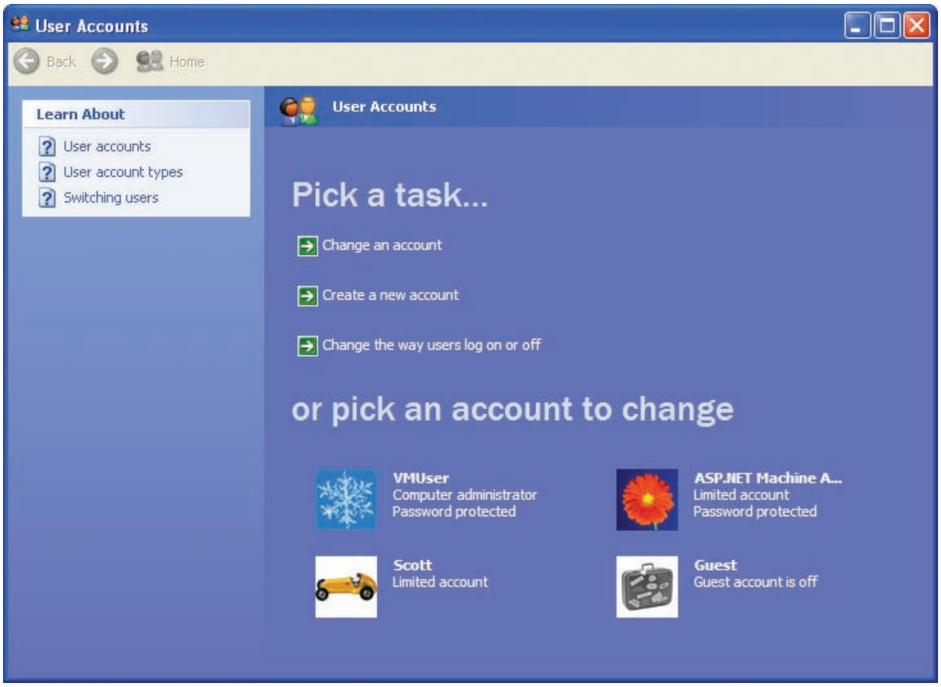
Simple Tools for Managing Users

While I've already covered some of what makes users and groups so powerful, Microsoft understood that everyday users wanted user accounts, too. Remember that, beyond all of the permissions and administrative privileges, user accounts also create personal folders for a user's files, such as his My Documents, My Photos, and My Music folders. To that end, every version and edition of Windows includes these simple tools for managing users, all of which are found in the Control Panel. You'll learn about a more advanced tool in the next section of this chapter.

Managing Users in Windows XP

Windows XP provides the **User Accounts applet** in the Control Panel for basic user and group management. Here you can create new users, delete users, change passwords, and so forth.

User Accounts hides the complete list of users using a simplistic reference to account types that is actually a reference to the user account's group membership. An account that is a member of the local Administrators group is called a **computer administrator**; an account that belongs only to the Local Users group is called a **limited user** account. Which users the applet displays depends on which type of user is currently logged on

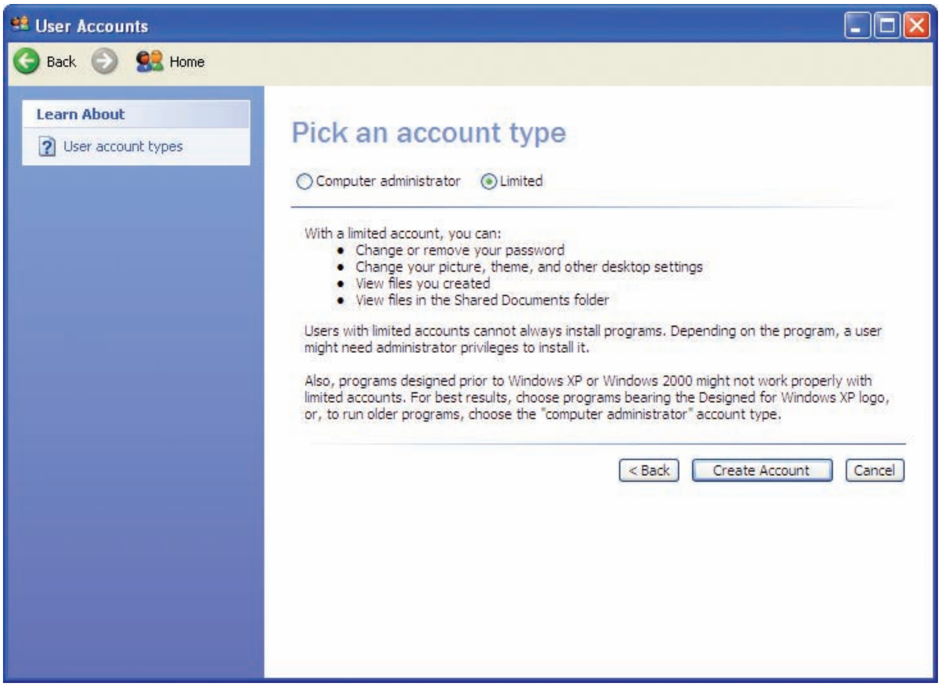


• **Figure 16.3** User Accounts dialog box showing a computer administrator, a couple of limited accounts, and the guest account (disabled)

(see Figure 16.3). When an administrator is logged on, the administrator sees both types of accounts and the guest account. Limited users see only their own account in User Accounts.

Windows XP requires you to create a second account that is a member of the Administrators group during the initial Windows installation. This is for simple redundancy—if one administrator is not available or is not able to log on to the computer, another one can.

Creating users is a straightforward process. You need to provide a user name (a password can and should be added later), and you need to know which type of account to create: computer administrator or limited. To create a new user in Windows XP, open the User Accounts applet from the Control Panel and click *Create a new account*. On the *Pick an account type* page, you can create either type of account (see Figure 16.4). Simply follow the prompts on the screen. After



Pick an account type

○ Computer administrator ● Limited

With a limited account, you can:

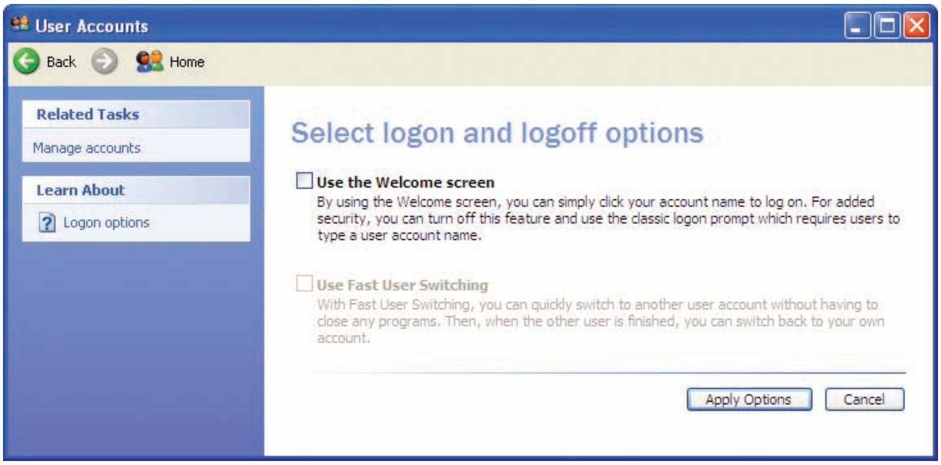
- Change or remove your password
- Change your picture, theme, and other desktop settings
- View files you created
- View files in the Shared Documents folder

Users with limited accounts cannot always install programs. Depending on the program, a user might need administrator privileges to install it.

Also, programs designed prior to Windows XP or Windows 2000 might not work properly with limited accounts. For best results, choose programs bearing the Designed for Windows XP logo, or, to run older programs, choose the "computer administrator" account type.

• **Figure 16.4** The Pick an account type page showing both options available you create your local accounts, you'll see them listed when you open the User Accounts applet.

Head back to the User Accounts applet and look at the *Change the way users log on and off* option. Select it to see two checkboxes (see Figure 16.5). If you select the *Use the Welcome screen* checkbox, Windows brings up the friendly **Welcome screen** shown in Figure 16.6 each time users log on. If this box is unchecked, you'll get the classic logon screen (see Figure 16.7).

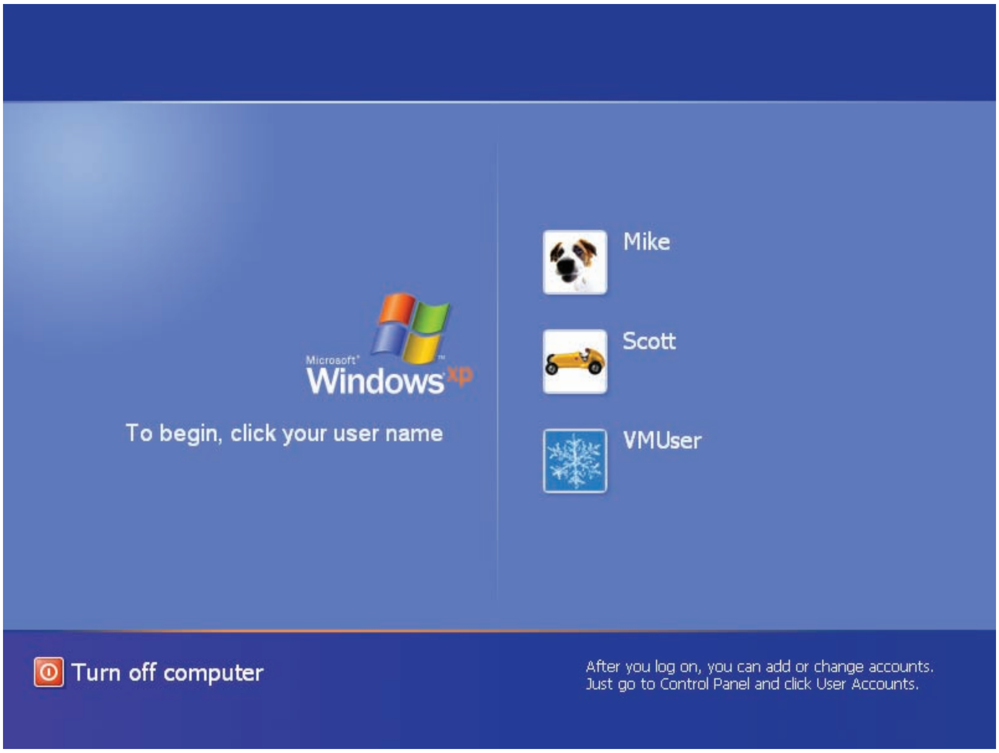


Select logon and logoff options

□ **Use the Welcome screen**
By using the Welcome screen, you can simply click your account name to log on. For added security, you can turn off this feature and use the classic logon prompt which requires users to type a user account name.

□ Use Fast User Switching
With Fast User Switching, you can quickly switch to another user account without having to close any programs. Then, when the other user is finished, you can switch back to your own account.

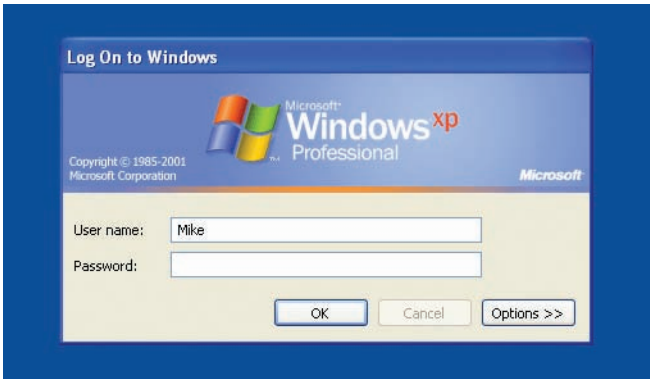
• **Figure 16.5** Select logon and logoff options



To begin, click your user name

After you log on, you can add or change accounts.
Just go to Control Panel and click User Accounts.

• **Figure 16.6** Welcome screen with three accounts


Log On to Windows

Microsoft Windows xp Professional
Copyright © 1985-2001 Microsoft Corporation
Microsoft

User name: Mike

Password:

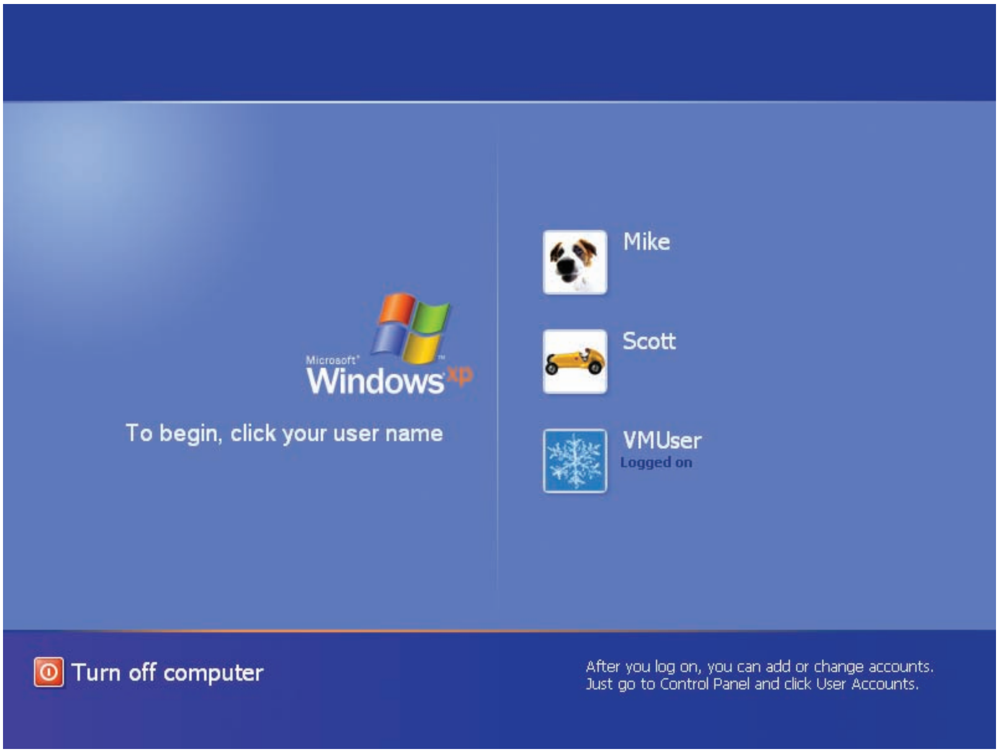
• Figure 16.7 Classic logon screen, XP style

The second option, Use Fast User Switching, enables you to switch to another user without logging off of the currently running user, a feature appropriately called **Fast User Switching**. This option is handy when two people actively share a system, or when someone wants to borrow your system for a moment but you don't want to close all of your programs. This option is only active if you have the *Use the Welcome screen* checkbox enabled. If Fast User Switching is enabled, when you click the Log Off button on the Start menu, you get the option to switch users, as shown in Figure 16.8.

Managing Users in Windows Vista

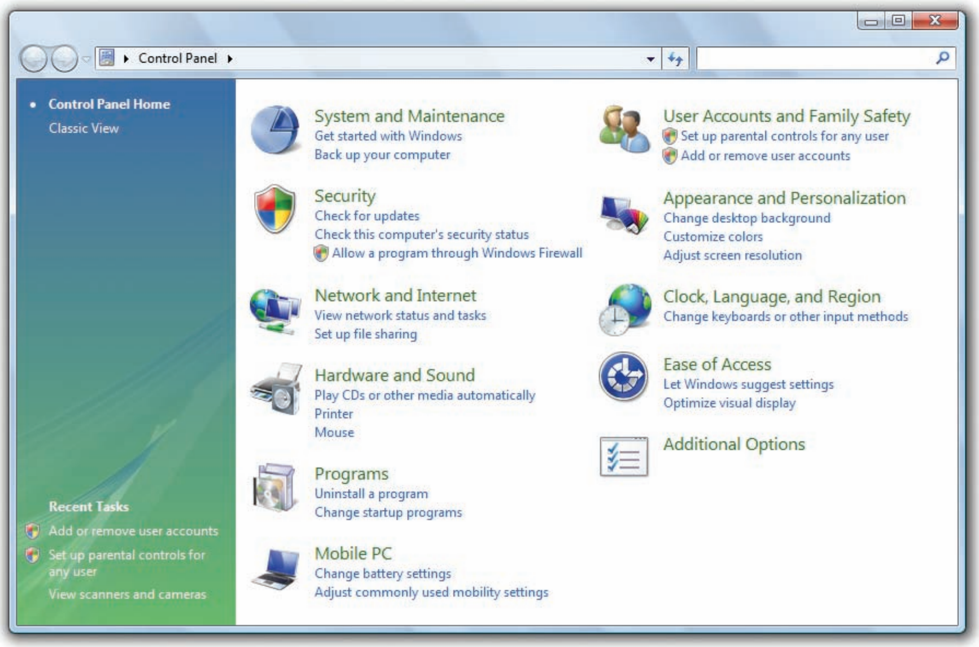
Microsoft made some major changes to user accounts and the applet used to create and modify them in Windows Vista. Just as with Windows XP, you create three accounts when you set up a computer: guest, administrator, and a local account that's a member of the Administrators group. That's about where the similarities end.

To add or modify a user account, you have numerous options depending on which Control Panel view you select and which edition and update of Vista you have installed. If your machine is on a workgroup, you'll see the User Accounts and Family Safety applet (see Figure 16.9). If you connect to a domain, the default Control Panel Home view offers the User Accounts applet (see Figure 16.10). The options in each applet differ as well, as you can see in the screenshots.

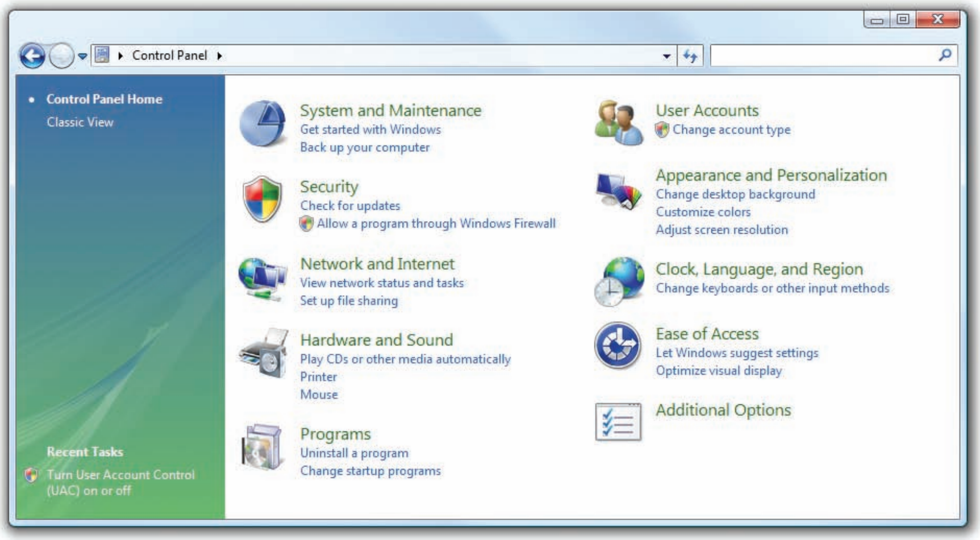

To begin, click your user name

After you log on, you can add or change accounts. Just go to Control Panel and click User Accounts.

• Figure 16.8 Switching users on the Welcome screen

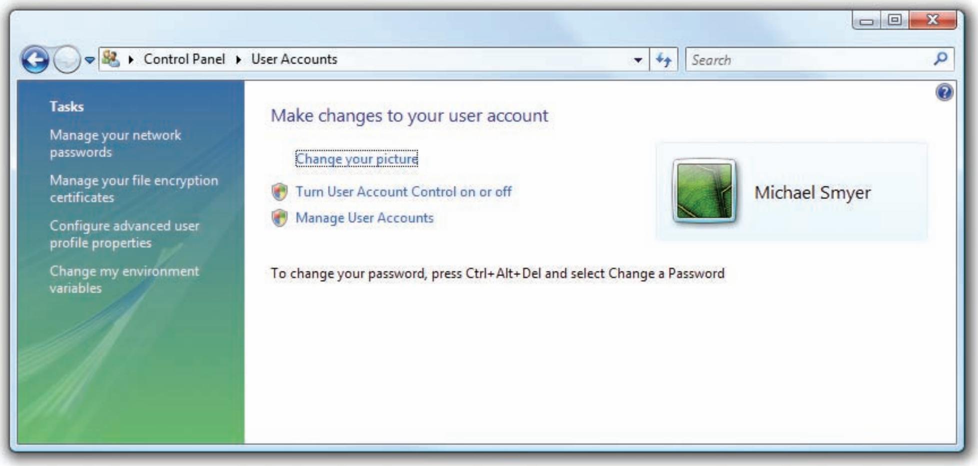

Control Panel
Control Panel Home
Classic View
Recent Tasks
Add or remove user accounts
Set up parental controls for any user
View scanners and cameras
System and Maintenance
Get started with Windows
Back up your computer
Security
Check for updates
Check this computer's security status
Allow a program through Windows Firewall
Network and Internet
View network status and tasks
Set up file sharing
Hardware and Sound
Play CDs or other media automatically
Printer
Mouse
Programs
Uninstall a program
Change startup programs
Mobile PC
Change battery settings
Adjust commonly used mobility settings
User Accounts and Family Safety
Set up parental controls for any user
Add or remove user accounts
Appearance and Personalization
Change desktop background
Customize colors
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods
Ease of Access
Let Windows suggest settings
Optimize visual display
Additional Options

• **Figure 16.9** User Accounts and Family Safety applet in the Control Panel Home in Windows Vista Home Premium



• **Figure 16.10** User Accounts applet in the Control Panel Home in Windows Vista Ultimate

Most techs almost immediately change the Control Panel view to Classic, but even there the different versions of Windows—and whether you're logged on to a workgroup or a domain—give you different versions of the User Accounts applet. Figure 16.11 shows the User Accounts applet in Windows Vista Business in a domain environment. Figure 16.12 shows the applet in Windows Vista Home Premium.



Control Panel ▸ User Accounts

Search

Tasks

Manage your network passwords

Manage your file encryption certificates

Configure advanced user profile properties

Change my environment variables

Make changes to your user account

Change your picture

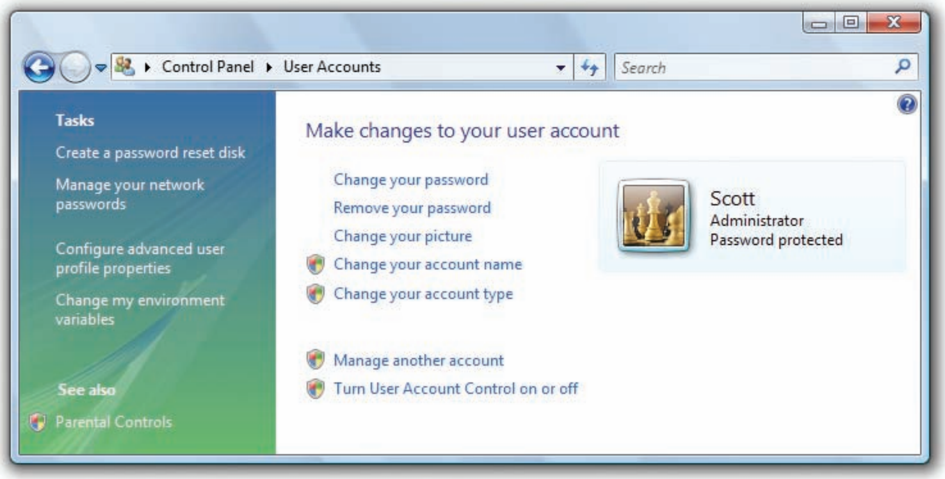
Turn User Account Control on or off

Manage User Accounts

Michael Smyer

To change your password, press Ctrl+Alt+Del and select Change a Password

• Figure 16.11 User Accounts applet in Windows Vista Business



Control Panel ▸ User Accounts

Search

Tasks

Create a password reset disk

Manage your network passwords

Configure advanced user profile properties

Change my environment variables

See also

Parental Controls

Make changes to your user account

Change your password

Remove your password

Change your picture

Change your account name

Change your account type

Manage another account

Turn User Account Control on or off

Scott
Administrator
Password protected

• Figure 16.12 User Accounts applet in Windows Vista Home Premium

The Tasks links on the left are similar between editions of Windows (with the addition of Parental Controls in the Home Premium edition), but the main options differ a lot. This chapter focuses on standalone machines, so we'll look more closely at the options included with Vista Home Premium.

Windows Vista Home Premium uses Vista's version of the Welcome screen for logging on, so each user account has a picture associated with it. You can change the picture from the User Accounts applet. You can also change the name of the user account here and alter the account type, demoting an account from administrator to standard user, for example.

To add a user in Windows Vista, open the User Accounts applet. You may need to open User Accounts and Family Safety first. Click *Manage another account* and select *Create a new account*. Give the account a user name and select a user account type. Then click Create Account.

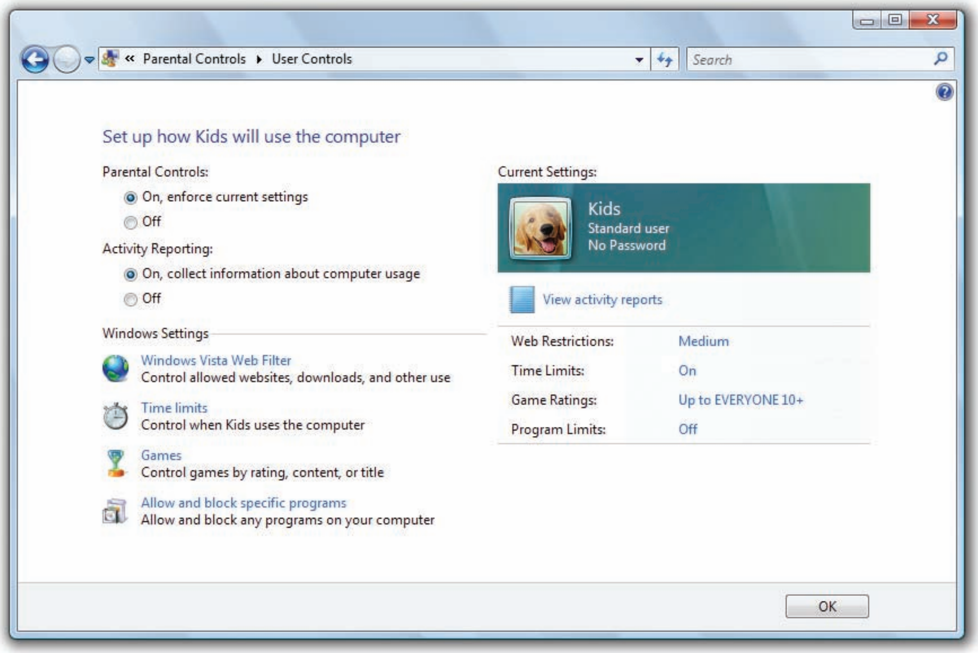
At least one account must be an administrator account. If you try to demote the sole administrator account, you'll find the option dimmed.

User Account Control Windows XP made it too easy—and, in fact, almost necessary—to make your primary account on a computer an administrator account. Because limited users can't do common tasks, such as running certain programs, installing applications, updating applications, updating Windows, and so on, most users simply created an administrator-level account and logged on. Such accounts have full control over the computer, so any malware that slipped in with the account could do a lot more harm.

Microsoft addressed this problem with the **User Account Control (UAC)**, a feature that enables standard users to do common tasks and provides a permissions dialog box when standard users *and* administrators do certain things that could potentially harm the computer (such as attempt to install a program). We'll discuss UAC in detail at the end of this chapter.

Parental Controls With **Parental Controls**, an administrator account can monitor and limit the activities of any standard user in Windows Vista (and Windows 7), a feature that gives parents and managers an excellent level of control over the content their children and employees can access (see Figure 16.13). Activity Reporting logs applications run or attempted to run, Web sites visited or attempted to visit, any kind of files downloaded, and more. You can block various Web sites by type or specific URL, or you can allow only certain Web sites, a far more powerful option.

Parental Controls enable you to limit the time that standard users can spend logged on. You can specify acceptable and unacceptable times of day when standard users can log on. You can restrict access both to types of games and to specific applications. If you like playing rather gruesome games filled with monsters and blood that you don't want your kids to play, for example, you can simply block any games with certain ESRB (Entertainment Software Rating Board) ratings, such as E for Everyone, T for Teen, or M for Mature or Mature 17+.



Set up how Kids will use the computer

Parental Controls:

● On, enforce current settings

○ Off

Activity Reporting:

● On, collect information about computer usage

○ Off

Windows Settings

Windows Vista Web Filter
Control allowed websites, downloads, and other use

Time limits
Control when Kids uses the computer

Games
Control games by rating, content, or title

Allow and block specific programs
Allow and block any programs on your computer

Current Settings:

Kids
Standard user
No Password

View activity reports

Web Restrictions:	Medium
Time Limits:	On
Game Ratings:	Up to EVERYONE 10+
Program Limits:	Off

• **Figure 16.13** Parental Controls

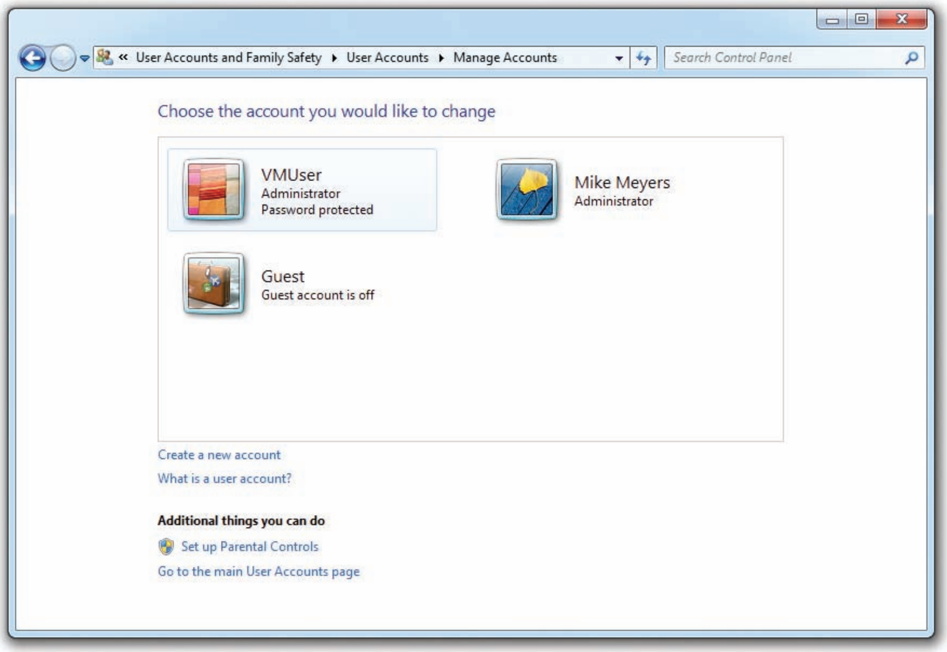
Managing Users in Windows 7

Windows 7 handles user creation in a manner very similar to Windows Vista, continuing the use of the User Accounts Control Panel applet. The Windows 7 applet is virtually identical to the one used in Windows Vista.

To create a user account, open the User Accounts applet and select *Manage another account* to see something like Figure 16.14.

Click on *Create a new account* to see your options for making a new account (see Figure 16.15). Note that this applet only enables you to make administrator accounts (in the Administrators group) or standard users (in the Users group).

While smaller, less sophisticated systems can get away with putting all their users into one of these two groups, you'll need to turn to Local Users and Groups to take full advantage of the power of Windows' users and groups.



« User Accounts and Family Safety ▸ User Accounts ▸ Manage Accounts

Search Control Panel

Choose the account you would like to change

VMUser
Administrator
Password protected

Mike Meyers
Administrator

Guest
Guest account is off

Create a new account

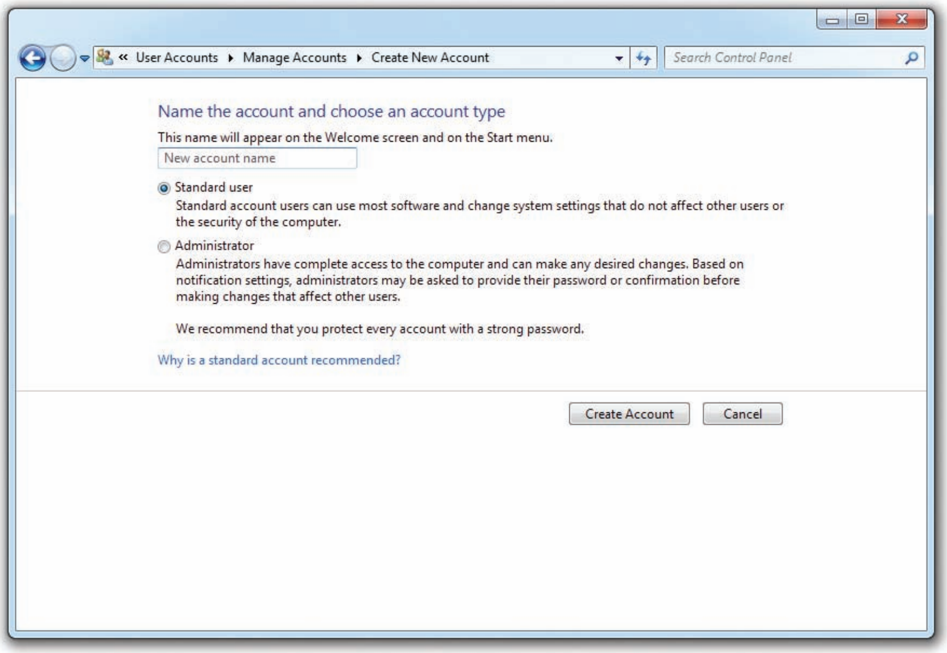
What is a user account?

Additional things you can do

Set up Parental Controls

Go to the main User Accounts page

• **Figure 16.14** Manage Accounts



« User Accounts ▸ Manage Accounts ▸ Create New Account

Search Control Panel

Name the account and choose an account type

This name will appear on the Welcome screen and on the Start menu.

New account name

● Standard user
Standard account users can use most software and change system settings that do not affect other users or the security of the computer.

○ Administrator
Administrators have complete access to the computer and can make any desired changes. Based on notification settings, administrators may be asked to provide their password or confirmation before making changes that affect other users.

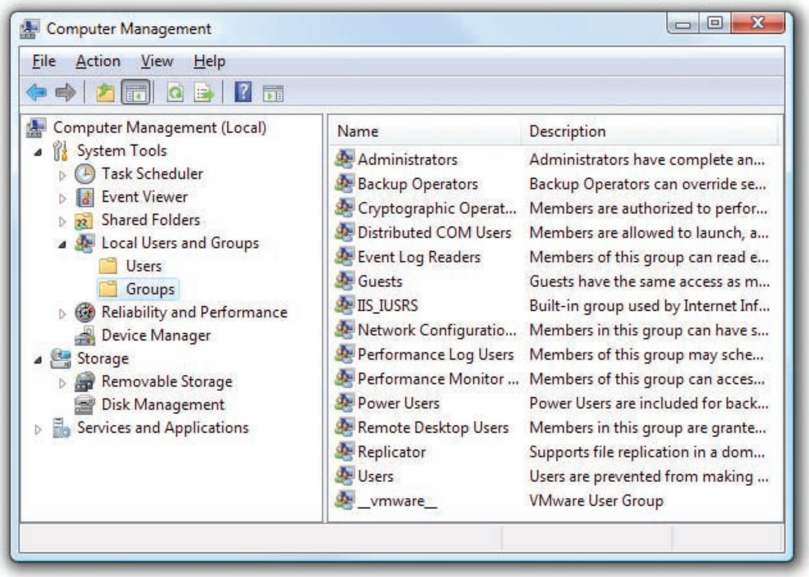
We recommend that you protect every account with a strong password.

Why is a standard account recommended?

• **Figure 16.15** Adding a new user

Advanced User Management

The professional editions of Windows include the **Local Users and Groups** tool, a more powerful tool for working with user accounts. You can get to Local Users and Groups via Control Panel | Administrative Tools | Computer Management. From here, you can create, modify, and remove users and groups. Keep in mind, however, that this advanced tool will not hold your hand like the Control Panel applets. Think of the Local Users and Groups tool as a bike without the training wheels of the User Accounts applet. Figure 16.16 shows the Local Users and Groups tool in Windows Vista with Groups selected.

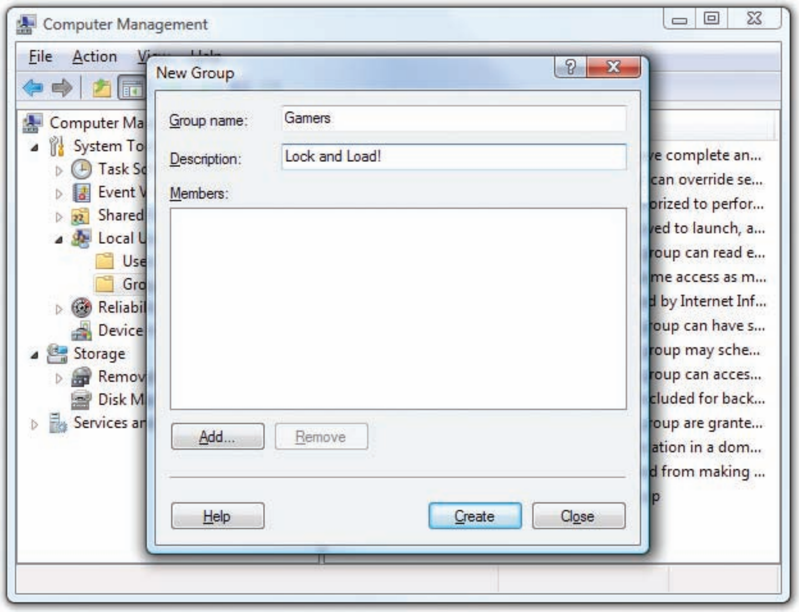


Name	Description
Administrators	Administrators have complete an...
Backup Operators	Backup Operators can override se...
Cryptographic Operat...	Members are authorized to perfor...
Distributed COM Users	Members are allowed to launch, a...
Event Log Readers	Members of this group can read e...
Guests	Guests have the same access as m...
IIS_IUSRS	Built-in group used by Internet Inf...
Network Configuratio...	Members in this group can have s...
Performance Log Users	Members of this group may sche...
Performance Monitor ...	Members of this group can acces...
Power Users	Power Users are included for back...
Remote Desktop Users	Members in this group are grante...
Replicator	Supports file replication in a dom...
Users	Users are prevented from making ...
__vmware__	VMware User Group

• **Figure 16.16** Local Users and Groups in Windows Vista

To add a group, simply right-click on a blank spot in the Groups folder and select New Group. This opens the New Group dialog box, where you can type in a group name and description in their respective fields (see Figure 16.17).

To add users to this group, click the Add button. The dialog box that opens varies a little in name among the three operating systems, though they all contain the same functionality (see Figure 16.18).

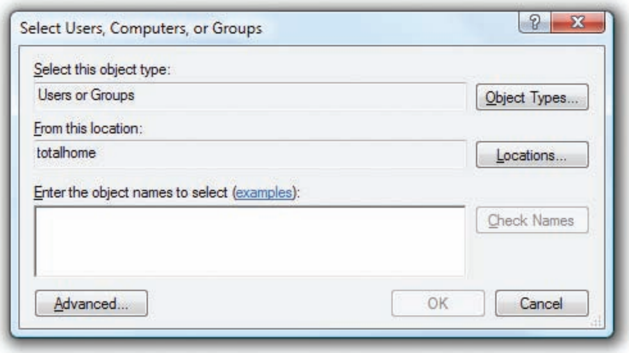


Group name: Gamers

Description: Lock and Load!

• **Figure 16.17** New Group dialog box in Windows Vista

You can add more than just users to a group. Windows uses multiple *object* types to define what you can add. Object types include user accounts, groups, and computers. Each object type can be added to a group and assigned permissions. The short story of how to add a user account is to click the Advanced button to expand the dialog box and then click the Find Now button (see Figure 16.19).

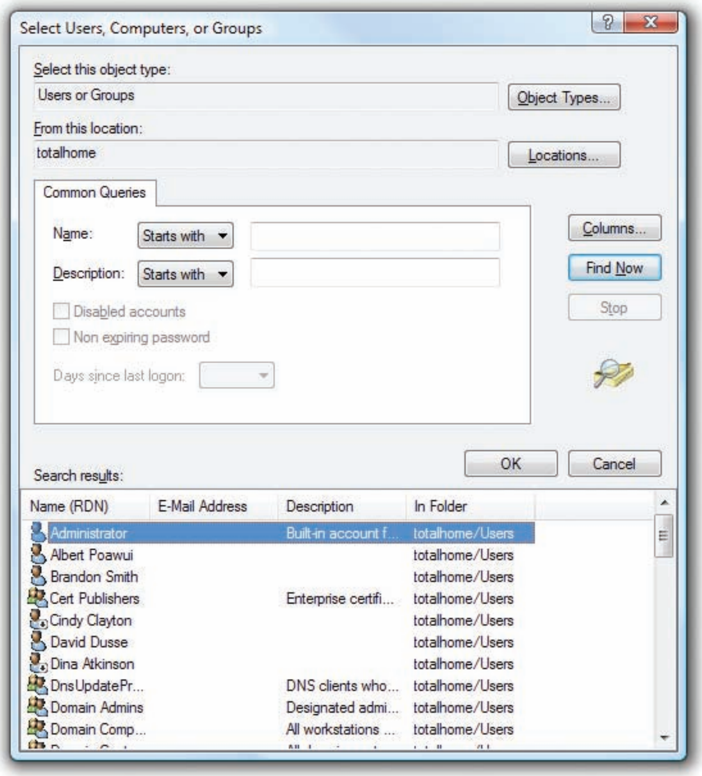

Select this object type: Users or Groups
From this location: totalhome
Enter the object names to select (examples):

• Figure 16.18 Select Users, Computers, or Groups dialog box in Windows Vista

You can either add group membership to a user's properties or add a user to a group's properties.

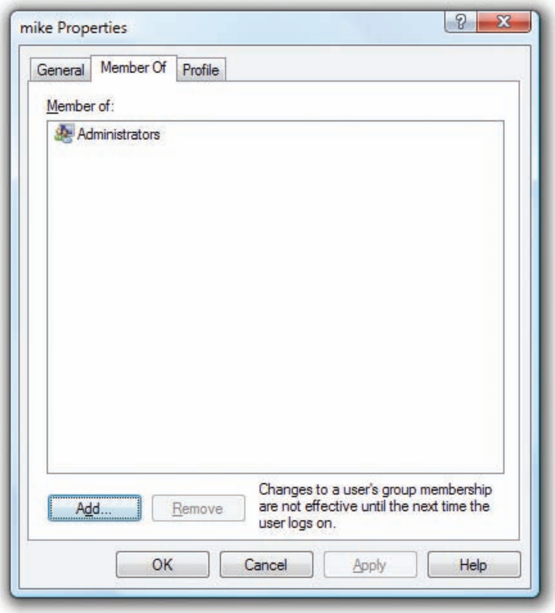
- To add group membership to a user account, select the Users folder, right-click a user account you want to change, and select Properties from the context menu. Then select the Member Of tab on the user account's Properties dialog box (see Figure 16.20). Click Add to add group membership.
- To add users via the group's properties, select the Groups folder. Right-click on a group and select Properties. Beneath the Members list, click the Add button to search for and add user accounts to the group.

You can also use either method to remove users. This level of flexibility makes the Local Users and Groups tool much more powerful and useful than the User Accounts Control Panel applets.


Select this object type: Users or Groups
From this location: totalhome
Name: Starts with
Description: Starts with
□ Disabled accounts
□ Non expiring password
Days since last logon:
Search results:

Name (RDN)	E-Mail Address	Description	In Folder
Administrator		Built-in account f...	totalhome/Users
Albert Poawui			totalhome/Users
Brandon Smith			totalhome/Users
Cert Publishers		Enterprise certifi...	totalhome/Users
Cindy Clayton			totalhome/Users
David Dusse			totalhome/Users
Dina Atkinson			totalhome/Users
DnsUpdatePr...		DNS clients who...	totalhome/Users
Domain Admins		Designated admi...	totalhome/Users
Domain Comp...		All workstations ...	totalhome/Users

• Figure 16.19 Select Users, Computers, or Groups dialog box with Advanced options expanded to show user accounts


Member of:
Administrators
Changes to a user's group membership are not effective until the next time the user logs on.

• Figure 16.20 Properties dialog box of a user account, where you can change group memberships for that account

Authorization Through NTFS

User accounts and passwords provide the foundation for securing a Windows computer, enabling users to authenticate onto a PC. After you've created a user account, you need to determine what the user can do with the available resources (files, folders, applications, and so on). We call this process *authorization*. Windows uses the powerful NT File System (NTFS) to protect its resources. Let's delve into the amazing world of NTFS to see how this powerful file system protects your folder and files.

NTFS Permissions

In Windows, every folder and file on an NTFS partition has a list that contains two sets of data. First, the list details every user and group that has access to that file or folder. Second, the list specifies the level of access that each user or group has to that file or folder. The level of access is defined by a set of restrictions called NTFS permissions. **NTFS permissions** define exactly what any particular account can or cannot do to the file or folder and are thus quite detailed and powerful. You can make it possible, for example, for a person to edit a file but not delete it. You can configure NTFS permissions to enable someone to create a folder and not allow other people to make subfolders.

Here are a few rules about NTFS permissions:

1. You may see the NTFS permissions on a folder or file by accessing the file's or folder's Properties dialog box and opening the Security tab.
2. NTFS permissions are assigned both to user accounts and groups, although it's considered a best practice to assign permissions to groups and then add user accounts to groups instead of adding permissions directly to individual user accounts.
3. Whoever creates a folder or a file has complete control over that folder or file.
4. Administrators do not automatically have complete control over every folder and file. If an administrator wants to access a folder or file they do not have permission to access, they may go through a process called Take Control.

✓ Cross Check

Creating NTFS

You learned a lot about NTFS back in Chapter 12, so dust off your memory and see if you can answer these questions. What tool do you use to create partitions and format them? How do you set the format type? How does FAT32 security stack up against NTFS security?

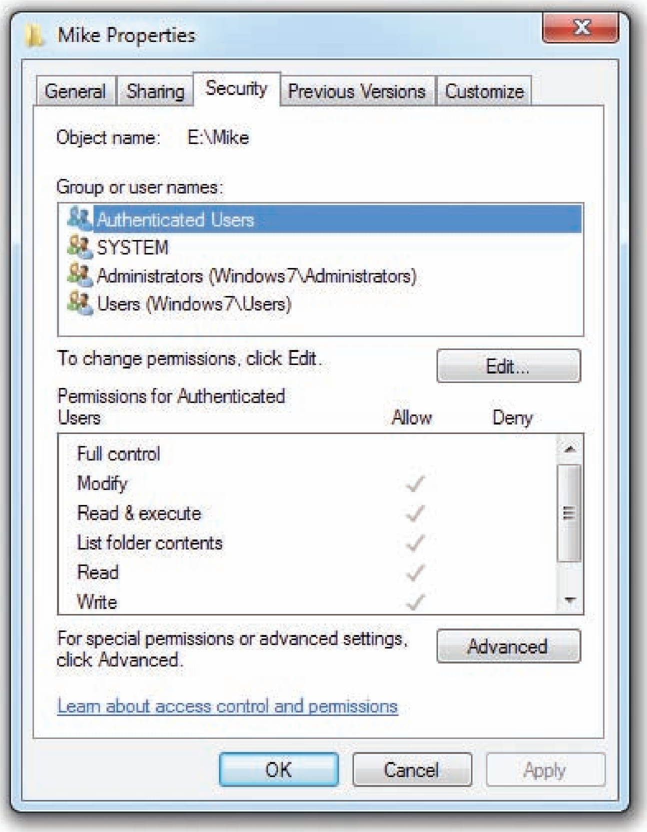
NTFS file and folder permissions are so complicated that entire books have been written on them! Fortunately, the CompTIA A+ 220-802 exam tests your understanding of only a few basic concepts of NTFS permissions: Ownership, Take Ownership permission, Change permission, folder permissions, and file permissions.

- **Ownership** When you create a new file or folder on an NTFS partition, you become the *owner* of that file or folder. Owners can do anything they want to the files or folders they own, including changing the permissions to prevent anybody, even administrators, from accessing them.
- **Take Ownership permission** With the **Take Ownership** special permission, anyone with the permission can seize control of a file or folder. Administrator accounts have Take Ownership permission for everything. Note the difference here between owning a file and accessing a file. If you own a file, you can prevent anyone from accessing that file. An administrator whom you have blocked, however, can take that ownership away from you and *then* access that file!
- **Change permission** Another important permission for all NTFS files and folders is the Change permission. An account with this permission can give or take away permissions for other accounts.
- **Folder permissions** Let's look at a typical folder on my Windows 7 system to see how this one works. My E: drive is formatted as NTFS, and on it I created a folder called E:\Mike. I set the permissions for the E:\Mike folder by right-clicking on the folder, selecting Properties, and clicking the Security tab (see Figure 16.21).
- **File permissions** File permissions are similar to Folder permissions. We'll talk about File permissions right after we cover Folder permissions.

In Windows, just about everything in the computer has a Security tab in its Properties dialog box, and every Security tab contains two main areas. The top area shows the list of accounts that have permissions for that resource. The lower area shows exactly what permissions have been assigned to the selected account.

Here are the standard permissions for a folder:

- **Full Control** Enables you to do anything you want.
- **Modify** Enables you to do anything except delete files or subfolders, change permissions, or take ownership.
- **Read & Execute** Enables you to see the contents of the folder and any subfolders.
- **List Folder Contents** Enables you to see the contents of the folder and any subfolders. (This permission seems the same as the Read & Execute permission, but it is only inherited by folders.)
- **Read** Enables you to view a folder's contents and open any file in the folder.
- **Write** Enables you to write to files and create new files and folders.



Object name: E:\Mike

Group or user names:

- Authenticated Users
- SYSTEM
- Administrators (Windows7\Administrators)
- Users (Windows7\Users)

To change permissions, click Edit.

Permissions for Authenticated Users	Allow	Deny
Full control		
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

• **Figure 16.21** The Security tab lets you set permissions.

File permissions are quite similar to folder permissions, with the main difference being the Special Permissions option, which I'll talk about a bit later in the chapter.

- **Full Control** Enables you to do anything you want.
- **Modify** Enables you to do anything except take ownership or change permissions on the file.
- **Read & Execute** Enables you to open files and applications.
- **Read** Enables you to open files.
- **Write** Enables you to open and write to the file.

Take some time to think about these permissions. Why would Microsoft create them? Think of situations where you might want to give a group Modify permission. Also, you can assign more than one permission. In many situations, we like to give users both the Read and Write permissions.

Permissions are cumulative. If you have Full Control on a folder and only Read permission on a file in the folder, you get Full Control permission on the file.

Don't panic about memorizing special permissions; just appreciate that they exist and that the permissions you see in the Security tab cover the vast majority of our needs.

Windows editions for home use have only a limited set of permissions you can assign. As far as folder permissions go, you can assign only one: Make This Folder Private. To see this in action, right-click a file or folder and select Sharing and Security from the options. Note that you can't just select Properties and see a Security tab as you can in the professional-oriented editions of Windows. Windows home editions do not have file-level permissions.

Permission Propagation

Permissions present an interesting challenge when you're moving and copying files. Techs need to understand what happens to permissions in several circumstances:

- Copying data within one NTFS-based partition
- Moving data within one NTFS-based partition
- Copying data between two NTFS-based partitions
- Moving data between two NTFS-based partitions
- Copying data from an NTFS-based partition to a FAT- or FAT32-based partition
- Moving data from an NTFS-based partition to a FAT- or FAT32-based partition

Do the permissions stay as they were on the original resource? Do they change to something else? Microsoft would describe the questions as such: Do inheritable permissions propagate? Ugh. CompTIA describes the process with the term **permission propagation**, which I take to mean "what happens to permissions on an object when you move or copy that object."

In Windows 7, if you access a folder's Properties dialog box, click on the Security tab, and then click the Advanced button, you'll see a little checkbox that says *Include inheritable permissions from this object's parent*. In other words, a user receives the parent folder's permissions for any files or subfolders created in that folder—a feature called **inheritance**. All versions of Windows have inheritance turned on by default, which most of the time is a good idea. However, there might be times where you want to turn off inheritance. Deselecting this option enables you to stop users from getting a specific permission via inheritance. Windows also provides explicit Deny functions for each option (see Figure 16.22). Deny overrules inheritance.

Let's look at our list of six things techs need to know to see what happens when you copy or move an object, such as a file or folder.

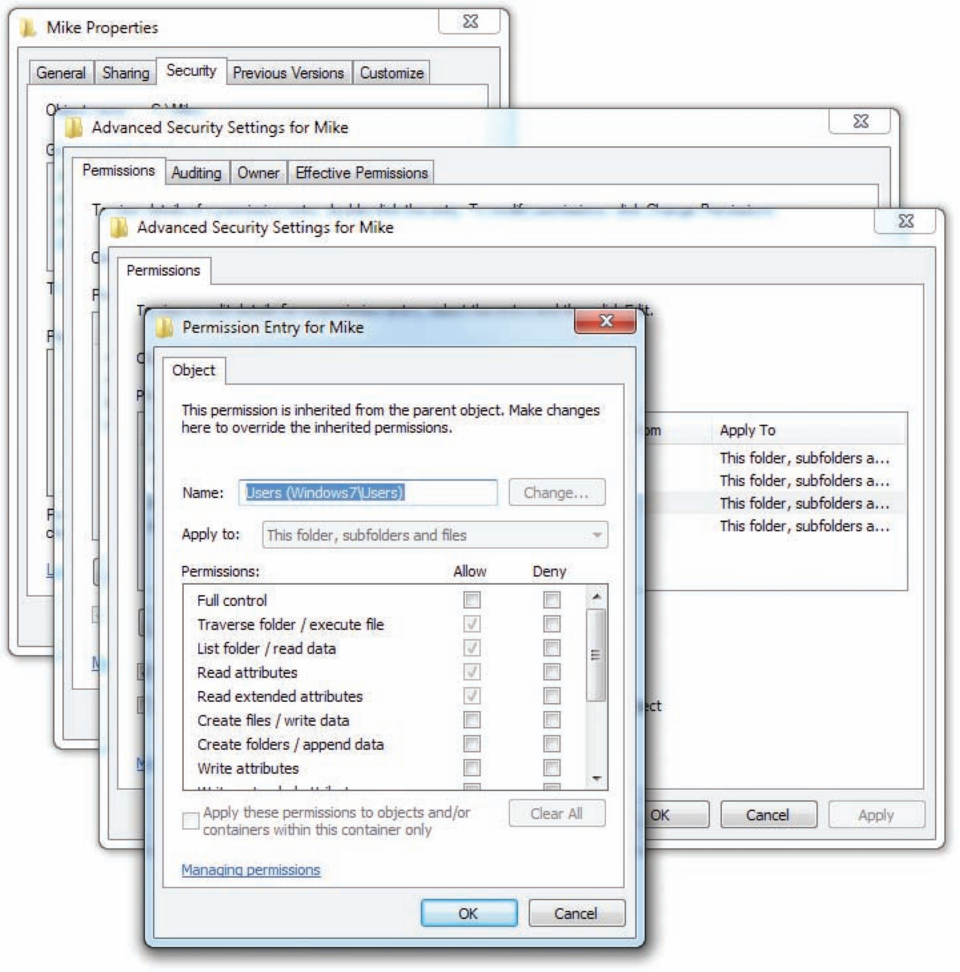
1. Copying within a partition creates two copies of the object. The object in the original location *retains* its permissions, unchanged. The copy of the object in the new location *inherits* the permissions from that new location. The new copy can have different permissions than the original.
2. Moving within a partition creates one copy of the object. That object *retains* its permissions, unchanged.
3. Copying from one NTFS partition to another creates two copies of the object. The object in the original location *retains* its permissions, unchanged. The copy of the object in the new location *inherits* the permissions from that new location. The new copy can have different permissions than the original.
4. Moving from one NTFS partition to another creates one copy of the object. The object in the new location *inherits* the permissions from that new location. The newly moved file can have different permissions than the original.

5. Copying from an NTFS-based partition to a FAT- or FAT32-based partition creates two copies of the object. The object in the original location *retains* its permissions, unchanged. The copy of the object in the new location has no permissions at all.
6. Moving from an NTFS-based partition to a FAT- or FAT32-based partition creates one copy of the object. That object has no permissions at all.

From a tech's standpoint, you need to be aware of how permissions can change when you move or copy files and, if in doubt about a sensitive file, check it before you sign off to a client. Having a top secret document totally locked down on a hard drive doesn't do you a lot of good if you put that document on a thumb drive to transport it and the thumb drive is FAT32!

Techs and Permissions

Techs, as a rule, hate NTFS permissions. You must have administrative privileges to do almost anything on a Windows machine, such as install updates, change drivers, and install applications; most administrators hate


Mike Properties
General
Sharing
Security
Previous Versions
Customize
Advanced Security Settings for Mike
Permissions
Auditing
Owner
Effective Permissions
Advanced Security Settings for Mike
Permissions
Apply To
This folder, subfolders a...
This folder, subfolders a...
This folder, subfolders a...
This folder, subfolders a...
OK
Cancel
Apply
Permission Entry for Mike
Object
Change...
Clear All
Managing permissions
OK
Cancel

This permission is inherited from the parent object. Make changes here to override the inherited permissions.

Name: Users (Windows7\Users)

Apply to: This folder, subfolders and files

Permissions:	Allow	Deny
Full control	☐	☐
Traverse folder / execute file	☑	☐
List folder / read data	☑	☐
Read attributes	☑	☐
Read extended attributes	☑	☐
Create files / write data	☐	☐
Create folders / append data	☐	☐
Write attributes	☐	☐

☐ Apply these permissions to objects and/or containers within this container only

• Figure 16.22 Special permissions

giving out administrative permissions (for obvious reasons). If an administrator does give you administrative permission for a PC, and something goes wrong with that system while you're working on it, you immediately become the primary suspect!

If you're working on a Windows system administered by someone else, make sure he understands what you are doing and how long you think it will take. Have the administrator create a new account for you that's a member of the Administrators group. Never ask for the password for a permanent administrator account! That way, you won't be blamed if anything goes wrong on that system: "Well, I told Janet the password when she installed the new hard drive…maybe she did it!" When you have fixed the system, *make sure the administrator deletes the account you used*.

This "protect yourself from passwords" attitude applies to areas other than just doing tech support on Windows. PC support folks get lots of passwords, scan cards, keys, and ID tags. New techs tend to get an "I can go anywhere and access anything" attitude, and this is dangerous. I've seen many jobs lost and friendships ruined when a backup suddenly disappears or a critical file gets erased. Everybody points to the support tech in these situations. In physical security situations, make other people unlock doors for you. In some cases, I've literally asked the administrator or system owner to sit behind me, read a magazine, and be ready to punch in passwords as needed. What you don't have access to can't hurt you.

Sharing a Windows PC Securely

User accounts, groups, and NTFS work together to enable you to share a Windows PC securely with multiple user accounts. You can readily share files, folders, programs, and more. More to the point, you can share only what should be shared, locking access to files and folders that you want to make private. Each version of Windows handles multiple user accounts and sharing among those accounts differently, so let's look at Windows XP, Windows Vista, and Windows 7 separately and then finish with a look at a few other sharing and security issues.

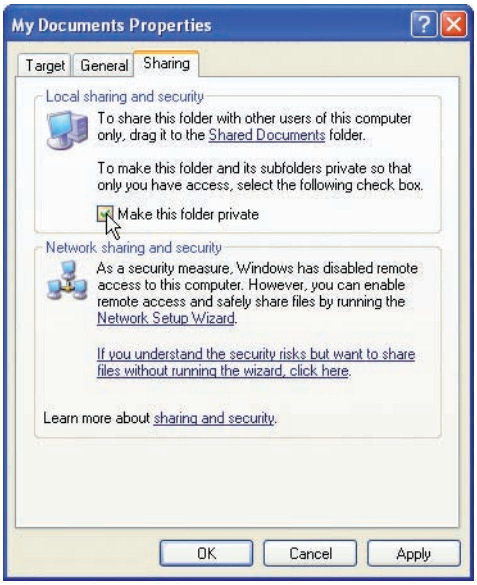
Sharing in Windows XP

Microsoft tried to make secure sharing in Windows XP easier than it was in previous versions of Windows. To this end, Microsoft included several features. Each user account gets a series of folders in My Documents that the user can share and administrators can access. Windows XP also comes with a set of pre-made folders called **Shared Documents** that are accessible by all of the users on the computer. Also, Windows XP comes with simple file sharing enabled by default, which makes the option to share or not pretty easy. Finally, Windows XP Professional provides the option to use the full NTFS permissions and make customized shares possible.

Making Personal Documents Secure

The fact that most users of Windows XP computers will be computer administrators rather than limited users creates a bit of an issue with computers shared by many users. By default, administrators can see all of the contents of Documents and Settings, where the My Documents folder for each user account resides. You can override this option in the My Documents Properties dialog box. Selecting the option to *Make this folder private* blocks the contents from anyone accessing them (see Figure 16.23).

Note that an administrator can take ownership of anything, so the only true way to lock down your data is to encrypt it. In the My Documents Properties dialog box, select the General tab and then click the Advanced button to open the Advanced Attributes dialog box. Click the checkbox next to *Encrypt contents to secure data* and that'll handle the encryption. Just make sure you have a password reset disk if you're going to use encryption to secure your files.



To share this folder with other users of this computer only, drag it to the Shared Documents folder.

To make this folder and its subfolders private so that only you have access, select the following check box.

☑ Make this folder private

As a security measure, Windows has disabled remote access to this computer. However, you can enable remote access and safely share files by running the Network Setup Wizard.

If you understand the security risks but want to share files without running the wizard, click here.

Learn more about sharing and security.

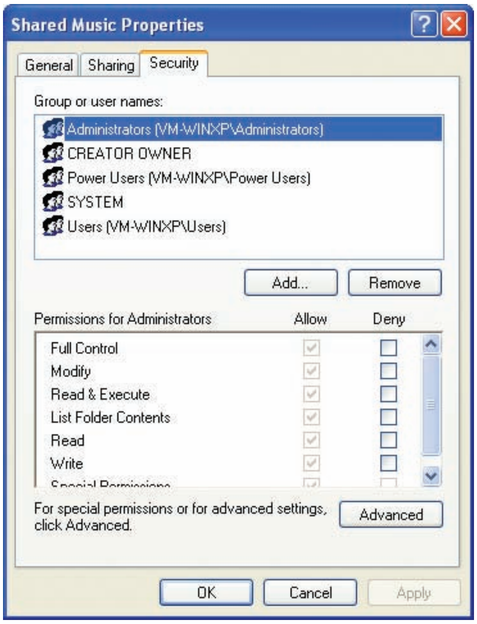
• **Figure 16.23** Making personal documents secure from prying eyes

Shared Documents

You can use the Shared Documents folders to move files and folders among many users of a single machine. Every account can access the Shared Documents folder and the subfolders within, such as Shared Music and Shared Pictures (see Figure 16.24). Because new folders inherit the permissions of parent folders, by default any new subfolder you create in Shared Documents can be accessed by any account.

Simple File Sharing

With **simple file sharing**, you essentially have one local sharing option, and that's to put anything you want to share into the Shared Documents folder or one of its subfolders. To share a folder over a network, you only have a couple of options as well, such as to share or not and, if so, to give full control to everybody. Note that the sharing option is enabled in Figure 16.25. It's pretty much all or nothing.



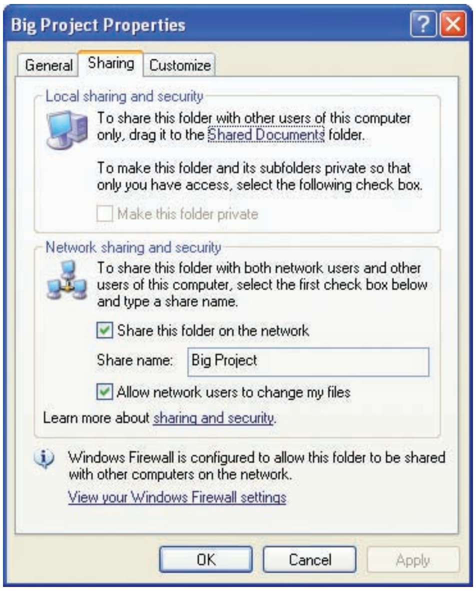
Group or user names:

- Administrators (VM-WINXP\Administrators)
- CREATOR OWNER
- Power Users (VM-WINXP\Power Users)
- SYSTEM
- Users (VM-WINXP\Users)

Permissions for Administrators	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□
Special Permissions	□	□

For special permissions or for advanced settings, click Advanced.

• **Figure 16.24** Shared Music Properties dialog box



To share this folder with other users of this computer only, drag it to the Shared Documents folder.

To make this folder and its subfolders private so that only you have access, select the following check box.

□ Make this folder private

To share this folder with both network users and other users of this computer, select the first check box below and type a share name.

☑ Share this folder on the network

Share name: Big Project

☑ Allow network users to change my files

Learn more about sharing and security.

Windows Firewall is configured to allow this folder to be shared with other computers on the network.

View your Windows Firewall settings

• **Figure 16.25** Folder shared, but seriously not secure

Windows XP Home and Media Center only give you the simple file sharing method, so the sharing of files and folders is straightforward. Windows XP Professional, on the other hand, enables you to turn off simple file sharing and unlock the true power of NTFS and permissions. To turn off simple file sharing, open a view of Windows Explorer (such as My Documents), choose Tools | Folder Options, and select the View tab. The very last option on the View tab is *Use simple file sharing (Recommended)*. Deselect that option, as in Figure 16.26, and then click OK.

When you add a Windows XP Professional system to a domain, simple file sharing is disabled. You must use the full power of NTFS.

When you access sharing and security now, you'll see a more fully formed security dialog box (see Figure 16.27).

Sharing in Windows Vista

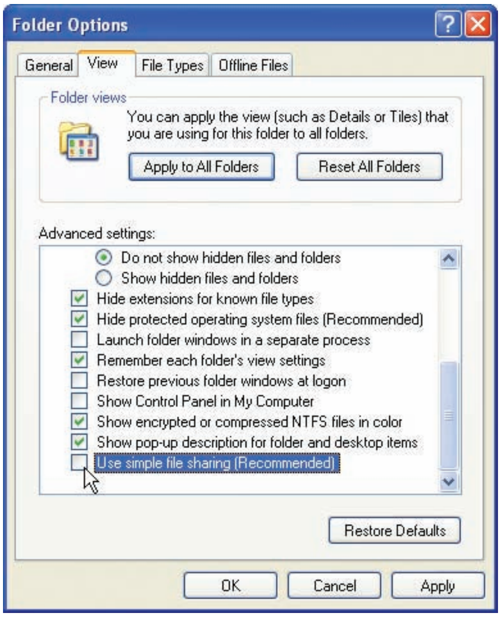
Microsoft tweaked the settings for sharing a single PC with multiple users in Windows Vista to fix the all-or-nothing approach offered by simple file sharing; Vista enables you to target shared files and folders to specific user accounts. Microsoft beefed up the standard user account (as you read about earlier in the chapter) so users could access what they needed to get meaningful work done. Plus they expanded the concept of the Shared Documents folder into the Public folders.

If the computer in question is on a Windows domain, the File Sharing dialog box differs such that you can search the network for user accounts in the domain. This makes it easy to share throughout the network.

Targeted Sharing

To share a folder or file with specific users—or with everyone, for that matter—you simply right-click on it and select Share. This opens the File Sharing dialog box, where you can select specific user accounts from a drop-down list (see Figure 16.28).

Once you select a user account, you can then choose what permission level to give that user. You have three choices: Reader, Contributor,



Folder Options

General | View | File Types | Offline Files

Folder views

You can apply the view (such as Details or Tiles) that you are using for this folder to all folders.

Apply to All Folders | Reset All Folders

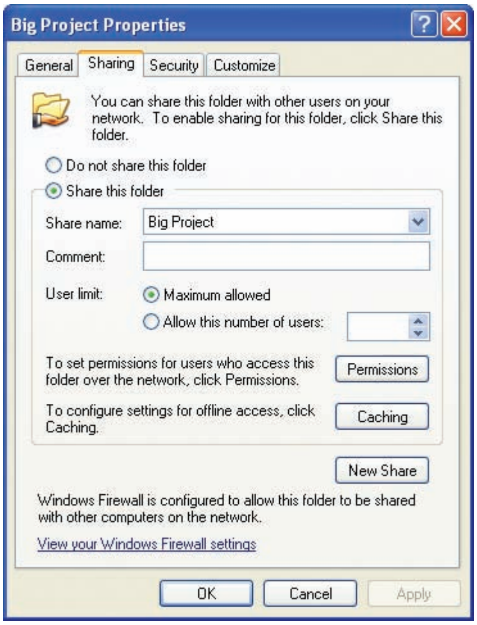
Advanced settings:

- ● Do not show hidden files and folders
- ○ Show hidden files and folders
- ☑ Hide extensions for known file types
- ☑ Hide protected operating system files (Recommended)
- ☐ Launch folder windows in a separate process
- ☑ Remember each folder's view settings
- ☐ Restore previous folder windows at logon
- ☐ Show Control Panel in My Computer
- ☑ Show encrypted or compressed NTFS files in color
- ☑ Show pop-up description for folder and desktop items
- ☐ Use simple file sharing (Recommended)

Restore Defaults

OK | Cancel | Apply

• Figure 16.26 Turning off simple file sharing



Big Project Properties

General | Sharing | Security | Customize

You can share this folder with other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: Big Project

Comment:

User limit: ● Maximum allowed
○ Allow this number of users:

To set permissions for users who access this folder over the network, click Permissions. | Permissions

To configure settings for offline access, click Caching. | Caching

New Share

Windows Firewall is configured to allow this folder to be shared with other computers on the network.

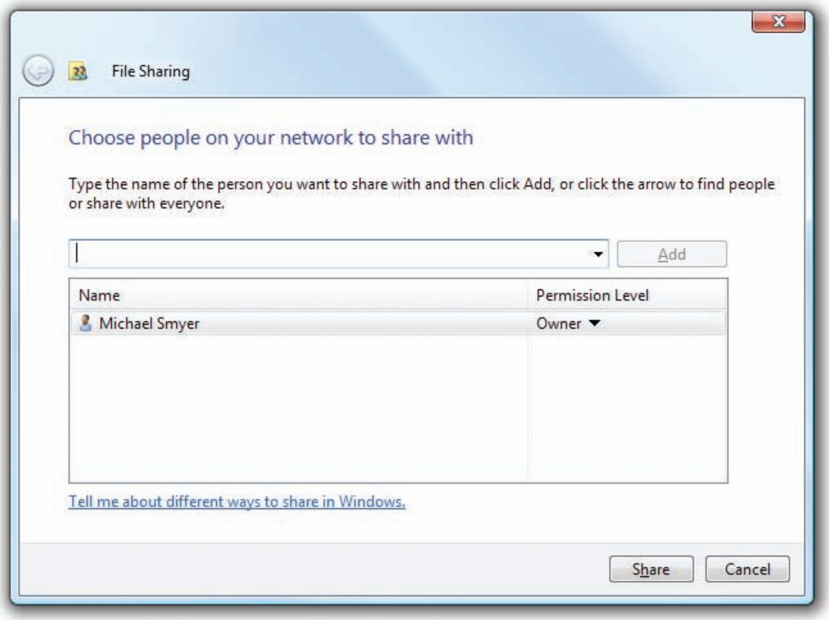
View your Windows Firewall settings

OK | Cancel | Apply

• Figure 16.27 Full sharing and security options in Windows XP or Co-owner (see Figure 16.29). *Reader* simply means the user has read-only permissions. *Contributor* gives the user read and write permissions and the permission to delete any file the user contributed to the folder. (Contributor only works at the folder level.) *Co-owner* enables the user to do anything.

Public Folders

Public folders offer another way to share files and folders. Anything you want to share with all other users on the local machine—or, if on a network, throughout the network—simply place it in the Public folder or one of the many subfolders, such as Public Documents or Public Pictures (see Figure 16.30). Note that the Public folder does not give you any control over what someone accessing the files contained within can do with those files.



Choose people on your network to share with

Type the name of the person you want to share with and then click Add, or click the arrow to find people or share with everyone.

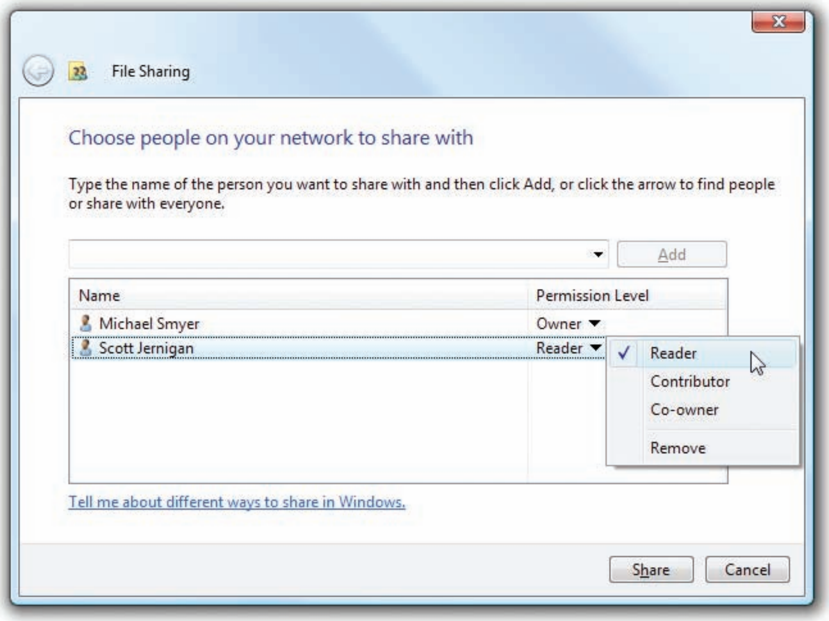
Name	Permission Level
Michael Smyer	Owner

• **Figure 16.28** File Sharing dialog box on a standalone machine

Like in Windows XP, NTFS sharing is alive and well in Windows Vista.

Sharing in Windows 7

Windows 7 keeps the file sharing options of Windows Vista and adds homegroups to the mix. You already learned all about homegroups in Chapter 5, but here's a quick refresher: Instead of sharing individual files or folders,

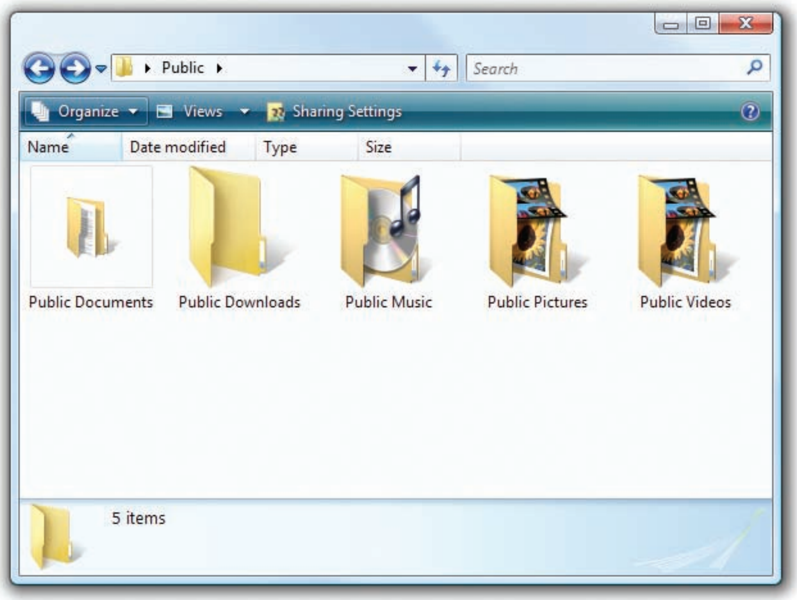


Choose people on your network to share with

Type the name of the person you want to share with and then click Add, or click the arrow to find people or share with everyone.

Name	Permission Level
Michael Smyer	Owner
Scott Jernigan	Reader

• **Figure 16.29** Permissions options



• Figure 16.30 Shared folders in the Public folder

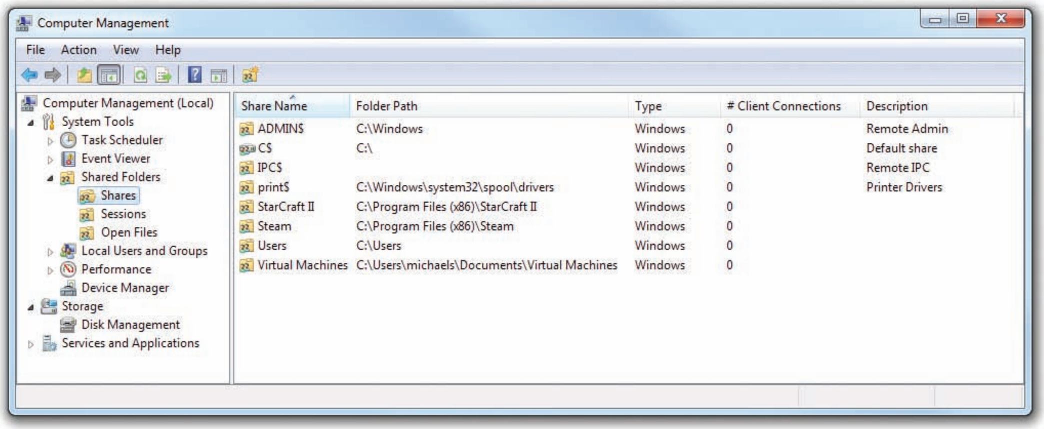
you can use HomeGroup to share libraries, such as your Documents or Music libraries. Any files in your shared libraries will be automatically accessible by everyone in the homegroup, though you can also use more specific permissions. You'll need a password to join a homegroup, so any shared data will be secure.

Locating Shared Folders

Before you walk away from a computer, you should check for any unnecessary or unknown (to you) shared folders on the hard drives. This enables you to make the computer as secure as possible for the user. When you open My Computer or Computer, shared folders don't just jump out at you, especially if they're buried deep within the file system. A shared C: drive is obvious, but a shared folder all the way down in D:\temp\backup\Simon\secret share would not be obvious, especially if none of the parent folders were shared.

Windows comes with a handy tool for locating all of the shared folders on a computer, regardless of where they reside on the drives. The Computer Management console in the Administrative Tools has a Shared Folders option under System Tools. In that are three options: Shares, Sessions, and Open Files. Select Shares to reveal all of the shared folders (see Figure 16.31).

You can double-click on any share to open the Properties dialog box for that folder. At that point, you can make changes to the share—such as users and permissions—just as you would from any other sharing dialog box.



Share Name	Folder Path	Type	# Client Connections	Description
ADMIN$	C:\Windows	Windows	0	Remote Admin
C$	C:\	Windows	0	Default share
IPC$		Windows	0	Remote IPC
print$	C:\Windows\system32\spool\drivers	Windows	0	Printer Drivers
StarCraft II	C:\Program Files (x86)\StarCraft II	Windows	0	
Steam	C:\Program Files (x86)\Steam	Windows	0	
Users	C:\Users	Windows	0	
Virtual Machines	C:\Users\michaels\Documents\Virtual Machines	Windows	0	

• Figure 16.31 Shared Folders tool in Computer Management

Administrative Shares

A close glance at the screenshot in Figure 16.31 might have left some of you with raised eyebrows and quizzical looks. What kind of share is ADMIN$ or C$?

Every version of Windows since Windows NT comes with several default shares, notably all hard drives—not optical drives or removable devices, such as thumb drives—plus the %systemroot% folder—usually C:\Windows—and a couple of others, depending on the system. These **administrative shares** give local administrators administrative access to these resources, whether they log on locally or remotely. (In contrast, shares added manually are called *local shares*.)

Administrative shares are odd ducks. You cannot change the default permissions on them. You can delete them, but Windows will re-create them automatically every time you reboot. They're hidden, so they don't appear when you browse a machine over the network, though you can map them by name. Keep the administrator password safe, and these default shares won't affect the overall security of the computer.

Administrative shares have been exploited by malware programs, especially because many users who set up their computers never give the administrator account a password. Starting with Windows XP Home, Microsoft changed the remote access permissions for such machines. If you log on to a computer remotely as administrator with no password, you get guest access rather than administrator access. That neatly nips potential exploits in the bud.

Protecting Data with Encryption

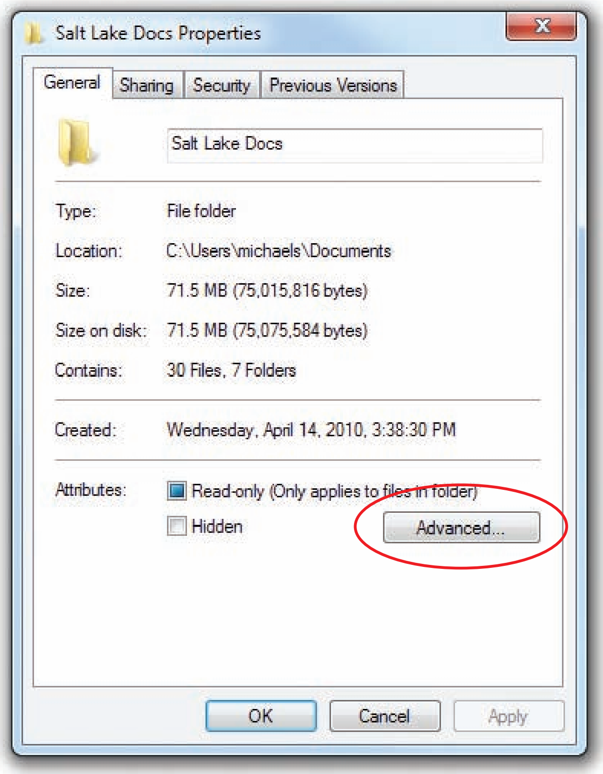
The scrambling of data through **encryption** techniques provides the only true way to secure your data from access by any other user. Administrators can use the Take Ownership permission to seize any file or folder on a computer, even those you don't actively share. Thus you need to implement other security measures for that data that needs to be ultra secure. Depending on the version of Windows, you have between zero and three encryptions tools: Windows Home editions (Windows XP Home Edition, Windows Vista Home Basic and Home Premium, and Windows 7 Home Premium) have basically no security features; Windows XP Professional uses the Encrypting File System to, well, encrypt files; and Windows Vista/7 Ultimate and Enterprise add an encryption system that can encrypt entire hard drives.

Encrypting File System

The professional editions of Windows (Windows XP Professional; Windows Vista Business, Ultimate, and Enterprise; and Windows 7 Professional, Ultimate, and Enterprise) offer a feature called the **Encrypting File System (EFS)**, an encryption scheme that any user can use to encrypt individual files or folders on a computer. The home editions of Windows do not enable encryption through the built-in tools, though you have the option to use third-party encryption methods, such as TrueCrypt, to lock down data.

To encrypt a file or folder takes but a moment. You right-click the file or folder you want to encrypt and select Properties. In the Properties dialog box for that object, select the General tab and click the Advanced button (see Figure 16.32) to open the Advanced Attributes dialog box. Click the checkbox next to *Encrypt contents to secure data* (see Figure 16.33). Click OK to close the Advanced Attributes dialog box and then click OK again on the Properties dialog box, and you've locked that file or folder from any user account aside from your own.

Encryption is just one possible *attribute* of a file. You can also make files hidden, read-only, and more, all from a file or folder's Properties dialog box. You'll learn more about attributes in Chapter 18.



Salt Lake Docs

Type: File folder

Location: C:\Users\michaels\Documents

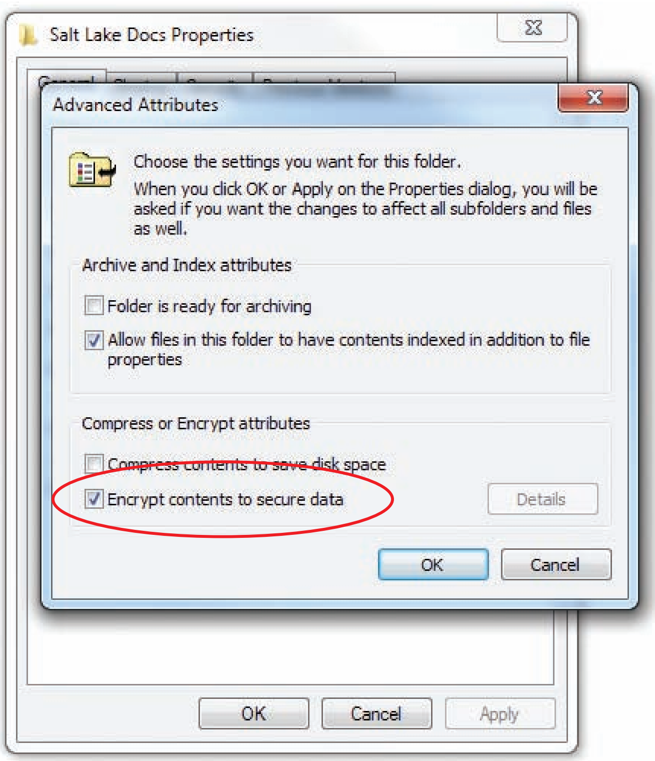
Size: 71.5 MB (75,015,816 bytes)

Size on disk: 71.5 MB (75,075,584 bytes)

Contains: 30 Files, 7 Folders

Created: Wednesday, April 14, 2010, 3:38:30 PM

Attributes: ■ Read-only (Only applies to files in folder)
□ Hidden



Choose the settings you want for this folder.

When you click OK or Apply on the Properties dialog, you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

□ Folder is ready for archiving

☑ Allow files in this folder to have contents indexed in addition to file properties

Compress or Encrypt attributes

□ Compress contents to save disk space

☑ Encrypt contents to secure data

• **Figure 16.32** Click the Advanced button on the General tab

• **Figure 16.33** Selecting encryption

Remember the password reset disk we discussed earlier in the chapter? If you use EFS, you simply must have a valid password reset disk in the event of some horrible catastrophe.

As long as you maintain the integrity of your password, any data you encrypt by using EFS is secure from prying. That security comes at a potential price, though, and your password is the key. The Windows security database stores the password (securely, not plain text, so no worries there), but that means access to your encrypted files is based on that specific installation of Windows. If you lose your password or an administrator resets your password, you're locked out of your encrypted files permanently. There's no recovery. Also, if the computer dies and you try to retrieve your data by installing the hard drive in another system, you're likewise out of luck. Even if you have an identical user name on the new system, the security ID that defines that user account will differ from what you had on the old system.

And one last caveat. If you copy an encrypted file to a disk formatted as anything but NTFS, you'll get a prompt saying that the copied file will not be encrypted. If you copy to a disk with NTFS, the encryption stays. The encrypted file—even if on a removable disk—will only be readable on your system with your login.

BitLocker Drive Encryption

Windows Vista/7's Ultimate and Enterprise editions offer full drive encryption through **BitLocker Drive Encryption**. BitLocker encrypts the whole drive, including every user's files, so it's not dependent on any one account. The beauty of BitLocker is that if your hard drive is stolen, such as in the case of a stolen portable computer, all of the data on the hard drive is safe. The thief can't get access, even if you have a user on that laptop that failed to secure his or her data through EFS.

BitLocker requires a special Trusted Platform Module (TPM) chip on the motherboard to function. The TPM chip validates on boot that the Vista/7 computer has not changed—that you still have the same operating system installed, for example, and that the computer wasn't hacked by some malevolent program. The TPM also works in cases where you move the BitLocker drive from one system to another.

If you have a legitimate BitLocker failure (rather than a theft) because of tampering or moving the drive to another system, you need to have a properly created and accessible recovery key or recovery password. The key or password is generally created at the time you enable BitLocker and should be kept somewhere secure, such as a printed copy in a safe or a file on a network server accessible only to administrators.

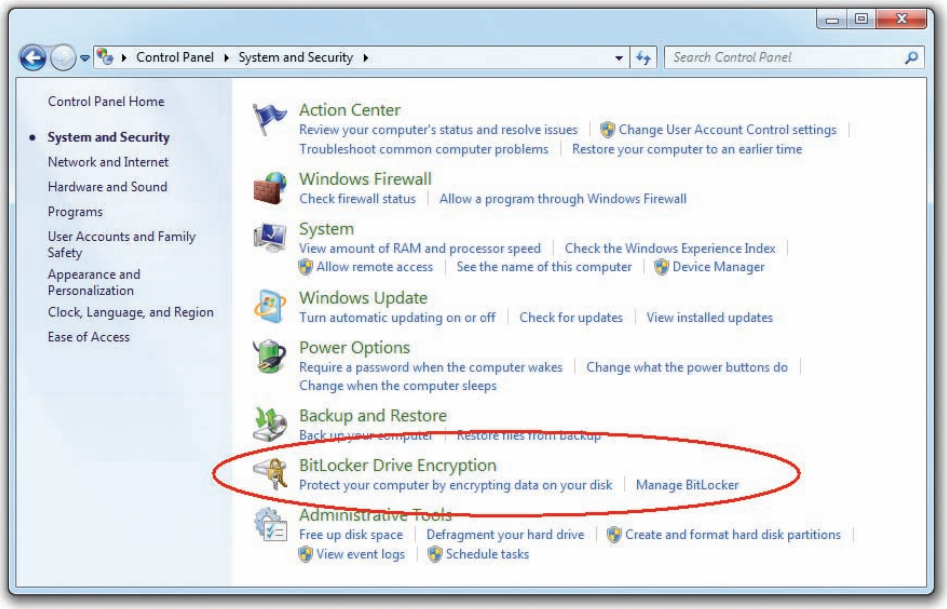
To enable BitLocker, double-click the BitLocker Drive Encryption icon in the Classic Control Panel, or select Security in Control Panel Home view and then click *Protect your computer by encrypting data on your disk* (see Figure 16.34).

Tech Tip

TrueCrypt

TrueCrypt is an open-source disk encryption application with versions available for just about every operating system. You can use TrueCrypt to encrypt an entire partition or you can create an encrypted volume into which you can securely store data. The beauty of the encrypted volume is that it acts like a folder that you can move around or toss on a USB flash drive. You can take the volume to another system and, as long as you have the password and TrueCrypt installed on the other system, read the contents of the encrypted volume. If the thumb drive is big enough, you can even put a copy of TrueCrypt on it and run the program directly from the thumb drive, enabling you to read the contents of the encrypted volume—as long as you know the proper password.

TrueCrypt has some limitations, such as a lack of support for dynamic disks and some problems with multiboot systems, but considering the price—free, though donations are cheerfully accepted—and the amazing power, it's hard not to love the program. This discussion of TrueCrypt barely scratches the surface of what the application can do, so check it out at www.truecrypt.org. If you're running Windows XP Home or Windows Vista/7 Home Premium, you can't get a better tool for securing your data.



Control Panel ▸ System and Security ▸

Search Control Panel

Control Panel Home
- System and Security
- Network and Internet
- Hardware and Sound
- Programs
- User Accounts and Family Safety
- Appearance and Personalization
- Clock, Language, and Region
- Ease of Access

Action Center
Review your computer's status and resolve issues | Change User Account Control settings | Troubleshoot common computer problems | Restore your computer to an earlier time

Windows Firewall
Check firewall status | Allow a program through Windows Firewall

System
View amount of RAM and processor speed | Check the Windows Experience Index | Allow remote access | See the name of this computer | Device Manager

Windows Update
Turn automatic updating on or off | Check for updates | View installed updates

Power Options
Require a password when the computer wakes | Change what the power buttons do | Change when the computer sleeps

Backup and Restore
Back up your computer | Restore files from backup

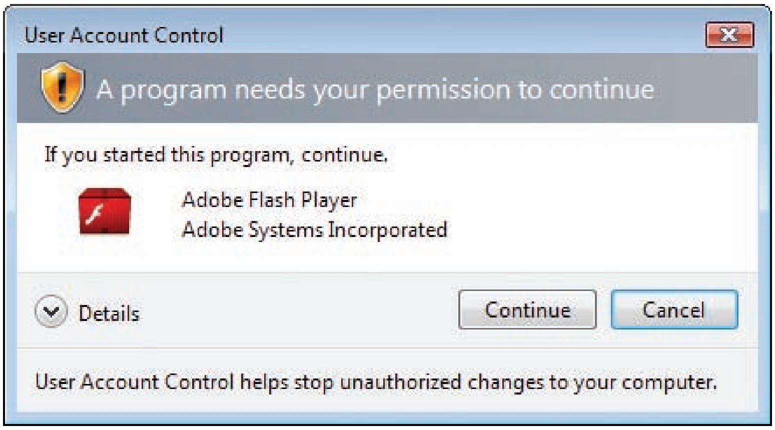
BitLocker Drive Encryption
Protect your computer by encrypting data on your disk | Manage BitLocker

Administrative Tools
Free up disk space | Defragment your hard drive | Create and format hard disk partitions | View event logs | Schedule tasks

• Figure 16.34 Enabling BitLocker Drive Encryption

User Account Control

When picking the poster child for the "327 Reasons We Hated Vista" list, I'll bet most folks put Vista's *User Account Control* (*UAC*) at the very top. Vista's UAC manifested as a pop-up dialog box that seemed to appear every time you tried to do *anything* on a Windows Vista system (see Figure 16.35).



User Account Control

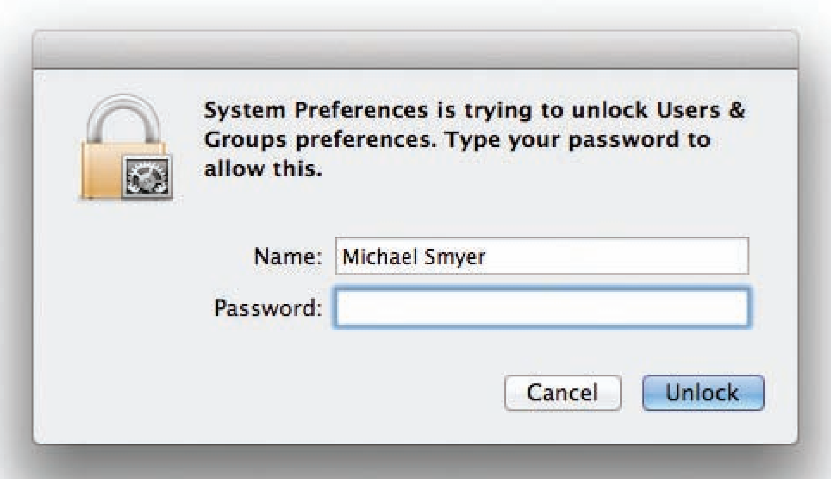
A program needs your permission to continue

If you started this program, continue.

Adobe Flash Player
Adobe Systems Incorporated

User Account Control helps stop unauthorized changes to your computer.

• Figure 16.35 UAC in action. Arrgh!



System Preferences is trying to unlock Users & Groups preferences. Type your password to allow this.

Name: Michael Smyer
Password:

• Figure 16.36 UAC equivalent on a Mac

It's too bad that UAC got such a bad rap. Not only is UAC an important security update for Windows Vista and Windows 7, but it is also a common feature in both Mac OS and Linux/Unix. Figure 16.36 shows the equivalent feature on a Mac.

If every other major operating system uses something like UAC, why was Microsoft slammed so hard when they unveiled UAC in Windows Vista? The reason is simple: Windows users are spoiled rotten, and, until UAC came along, the vast majority of users had no idea how risky their computing behavior was.

The problem started years ago when Microsoft created NTFS. NTFS uses robust user accounts and enables fine control over how users access files and folders—but at a cost: NTFS in its pure form is somewhat complicated. To share a folder, you need to make sure the person accessing that folder has a user account and that you've configured the NTFS permissions to give that user the permissions needed to do whatever he or she wants to do (see Figure 16.37).

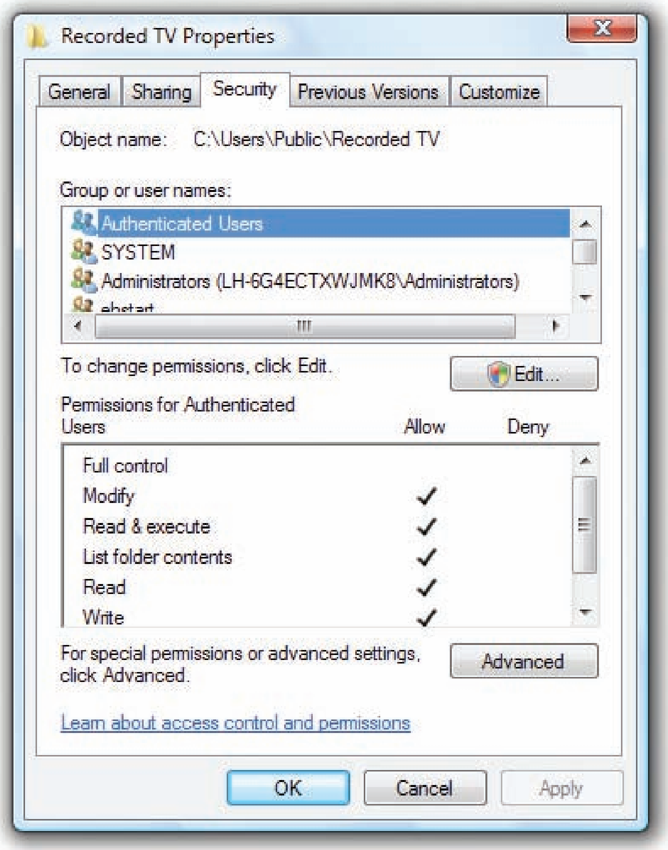
User accounts have always been a bit of a challenge. The only account that can truly do *anything* on a Windows system is the administrator. Sure, you can configure a system with groups and assign NTFS permissions to those groups—and this is commonly done on large networks with a full-time IT staff—but what about small offices and home networks? These users almost never have the skill sets to deal with the complexities of users and groups, which often results in systems where the user accounts are all assigned administrator privileges by default—and that's when it gets dangerous (see Figure 16.38).

UAC in Windows Vista

User Account Control enables users to know when they are about to do something that has serious consequences. The Microsoft TechNet library

("Understanding and Configuring User Account Control in Windows Vista") provides examples of common actions that require Administrator privileges:

- Installing and uninstalling applications
- Installing a driver for a device (e.g., a digital camera driver)
- Installing Windows Updates
- Configuring Parental Controls
- Installing an ActiveX control
- Adjusting Windows Firewall settings
- Changing a user's account type
- Modifying UAC settings in the Security Policy Editor snap-in (secpol.msc)
- Configuring Remote Desktop access
- Adding or removing a user account
- Coping or moving files into the Program Files or Windows directory
- Scheduling Automated Tasks
- Restoring system backed-up files
- Configuring Automatic Updates
- Browsing to another user's directory



Object name: C:\Users\Public\Recorded TV

Group or user names:

Authenticated Users
SYSTEM
Administrators (LH-6G4ECTXWJMK8\Administrators)
ebstart

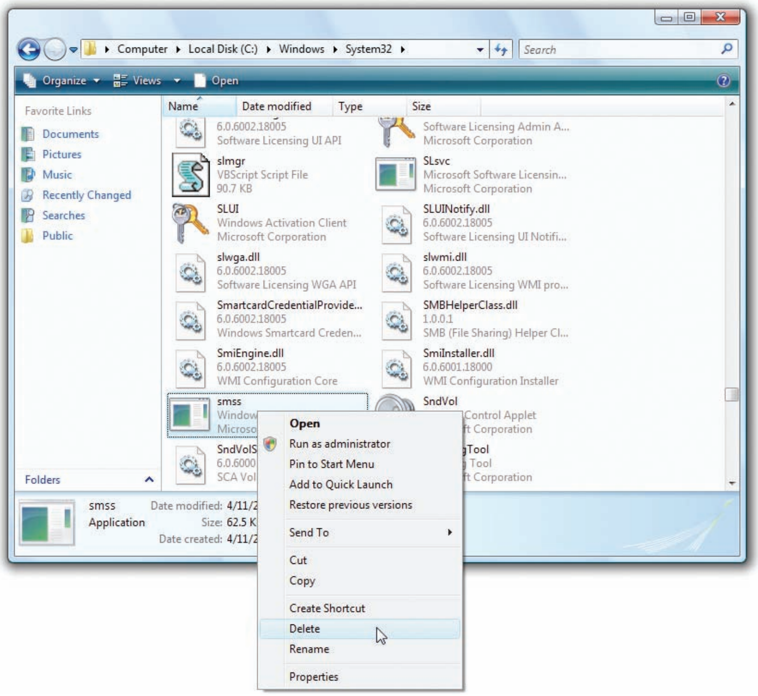
To change permissions, click Edit.

Permissions for Authenticated Users	Allow	Deny
Full control		
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

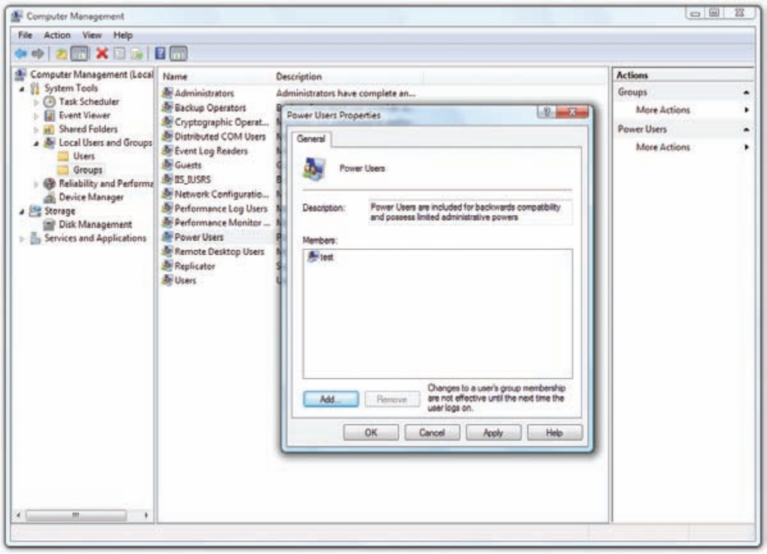
For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

• Figure 16.37 Typically confusing settings for NTFS permissions



• Figure 16.38 The danger of administrator privileges in the wrong hands!



Administrators have complete an...

Power Users are included for backwards compatibility and possess limited administrative powers

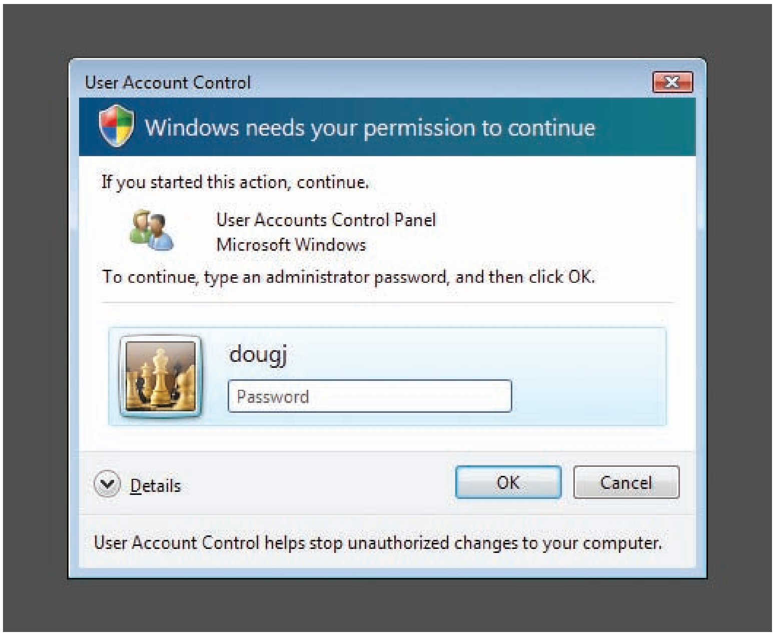
Changes to a user's group membership are not effective until the next time the user logs on.

• **Figure 16.39** Power Users group—almost never used at the small office/home level

Before Vista, Microsoft invented the idea of the Power Users group to give users almost all of the power of an administrator account (to handle most of the situations just described) without actually giving users the full power of the account. Assigning a user to the Power Users group still required someone who knew how to do this, however, so most folks at the small office/home level simply ignored the Power Users group (see Figure 16.39).

Clearly, Microsoft needed a better method to prevent people from running programs that they should not run. If users have the correct privileges, however—or the ability to "escalate" their privileges to that of an administrator—then they should be able to do what they need to do as simply as possible. Microsoft needed to make the following changes:

- The idea of using an administrator account for daily use needed to go away.
- Any level of account should be able to do anything as easily as possible.
- If a regular account wants to do something that requires administrator privileges, the user of the regular account will need to enter the administrator password.
- If a user with administrator privileges wants to run something that requires administrator privileges, the user will not have to reenter his or her password, but the user will have to respond to an "Are you sure?"-type dialog box so he or she appreciates the gravity of the action—thus, the infamous UAC dialog box.



Windows needs your permission to continue

If you started this action, continue.

User Accounts Control Panel
Microsoft Windows

To continue, type an administrator password, and then click OK.

dougj

Password

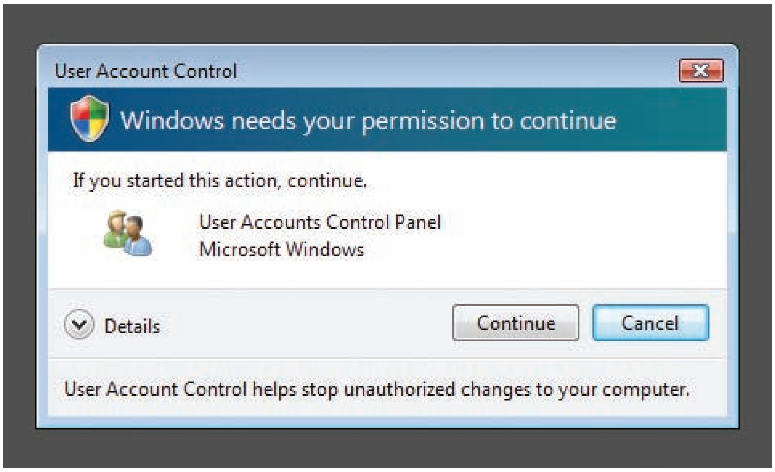
User Account Control helps stop unauthorized changes to your computer.

• **Figure 16.40** Prompting for an administrator password in Vista

How UAC Works

UAC works for both standard user accounts and administrator accounts. If a standard user attempts to do something that requires administrator privileges, he or she sees a UAC dialog box that prompts for the administrator password (see Figure 16.40).

If a user with administrator privileges attempts to do something that requires administrator privileges, a simpler UAC dialog box appears, like the one shown in Figure 16.41.



User Account Control

Windows needs your permission to continue

If you started this action, continue.

User Accounts Control Panel
Microsoft Windows

User Account Control helps stop unauthorized changes to your computer.

• **Figure 16.41** Classic UAC prompt

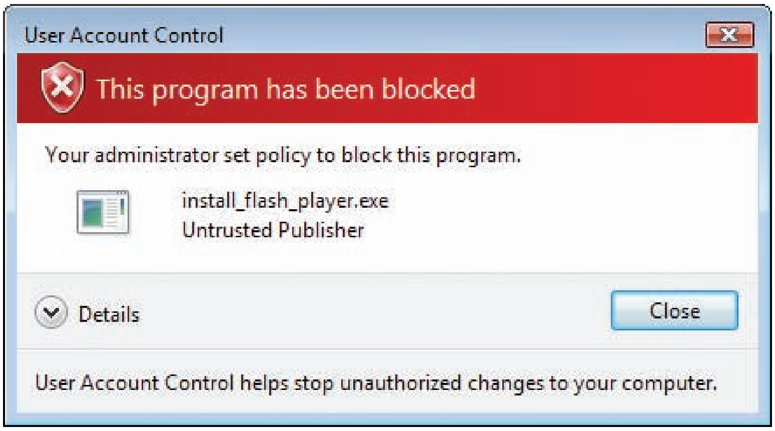
Interestingly, Vista has not one but four different UAC prompts, depending on the program/feature you wish to run, as outlined in Table 16.1.

The official name for the UAC dialog box is the "UAC consent prompt." When the UAC consent prompt appears in Vista, the rest of the desktop darkens and you cannot take any other action until you respond to the consent prompt.

Table 16.1 UAC Prompts in Windows Vista

UAC Classification	Type of Program
Blocked	A program that has been blocked by a security policy
Unverified	An unknown third-party program
Verified	A digitally signed, third-party program or non-core OS program
Published by Vista	A program that is a core part of the operating system

Blocked programs generate a scary-looking, red-bannered dialog box like the one shown in Figure 16.42. Note you can click OK in Windows Vista (or Close in Windows 7) or look at more details (if available).



User Account Control

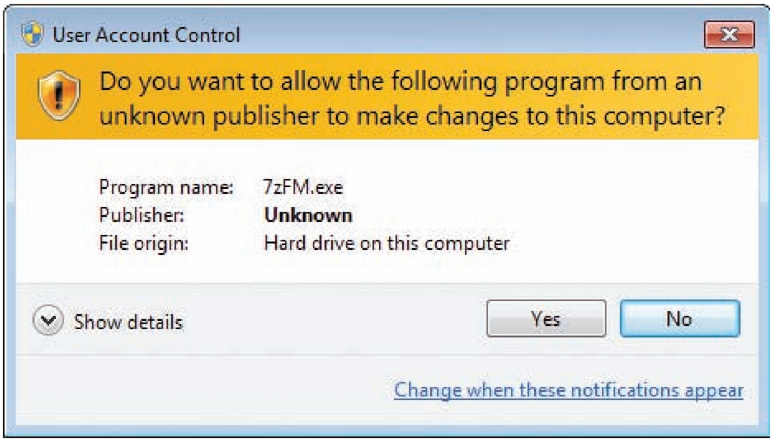
This program has been blocked

Your administrator set policy to block this program.

install_flash_player.exe
Untrusted Publisher

User Account Control helps stop unauthorized changes to your computer.

• **Figure 16.42** Blocked program

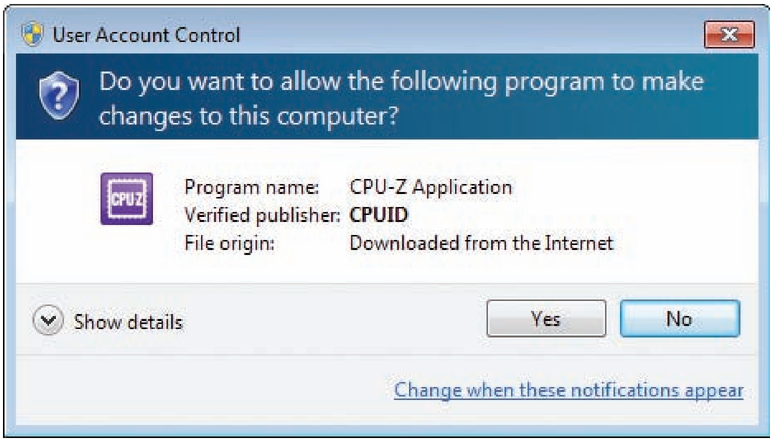


User Account Control

Do you want to allow the following program from an unknown publisher to make changes to this computer?

Program name: 7zFM.exe
Publisher: **Unknown**
File origin: Hard drive on this computer

• **Figure 16.43** Unverified program



User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: CPU-Z Application
Verified publisher: **CPUID**
File origin: Downloaded from the Internet

• **Figure 16.44** Verified program

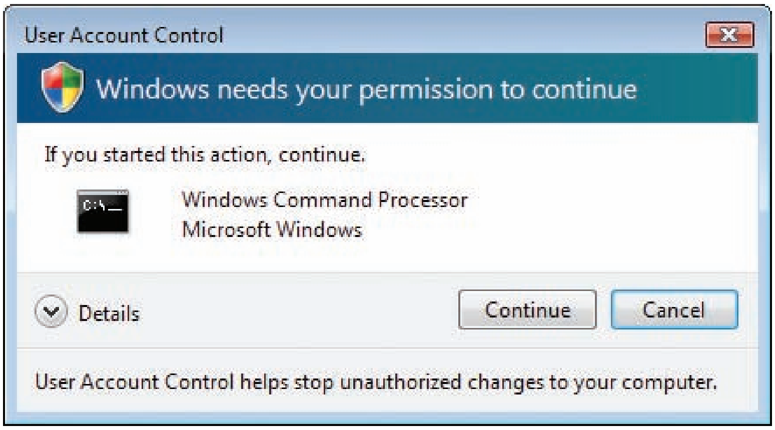
Unverified programs lack any form of certificate to validate. In this case, you get a yellow-bannered dialog box warning you the application is unsigned and giving you two options: allow the program to run (Yes) or not (No). See Figure 16.43 for an example of this.

Verified programs aren't part of the core of Vista and are usually written by third parties. These programs do have valid, verified certificates. You can identify the dialog box by its gray-blue banner (see Figure 16.44).

Published by Vista programs are written as part of the core of Vista and show up with a teal-bannered dialog box (see Figure 16.45).

UAC uses small shield icons to warn you ahead of time that it will prompt you before certain tasks, as shown in Figure 16.46. Microsoft updated this somewhat redundant feature in Windows 7, as you'll soon see.

UAC gives users running a program an opportunity to consider their actions before they move forward. It's a good thing, but spoiled Windows users aren't accustomed to something that makes them consider their actions. As a result, one of the first things everyone learned how to do when Vista came out was to turn off UAC.



User Account Control

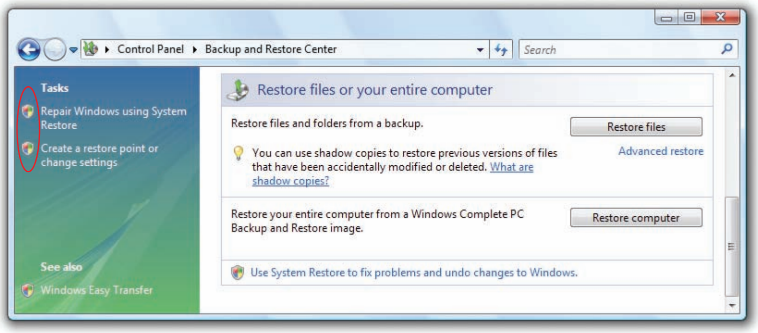
Windows needs your permission to continue

If you started this action, continue.

Windows Command Processor
Microsoft Windows

User Account Control helps stop unauthorized changes to your computer.

• **Figure 16.45** Published by Vista


Control Panel ▸ Backup and Restore Center
Search
Tasks
Repair Windows using System Restore
Create a restore point or change settings
See also
Windows Easy Transfer
Restore files
Advanced restore
Restore computer

Restore files or your entire computer

Restore files and folders from a backup.

You can use shadow copies to restore previous versions of files that have been accidentally modified or deleted. What are shadow copies?

Restore your entire computer from a Windows Complete PC Backup and Restore image.

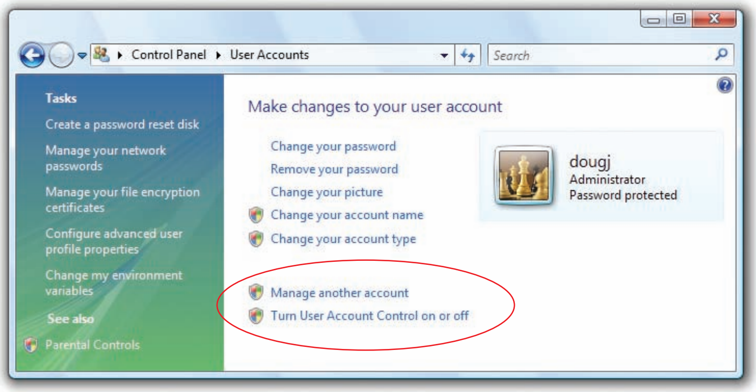
Use System Restore to fix problems and undo changes to Windows.

• **Figure 16.46** Shield icons in the Control Panel

How to Turn Off UAC

You can turn off UAC in a number of ways in Windows. Here are the two most common ways:

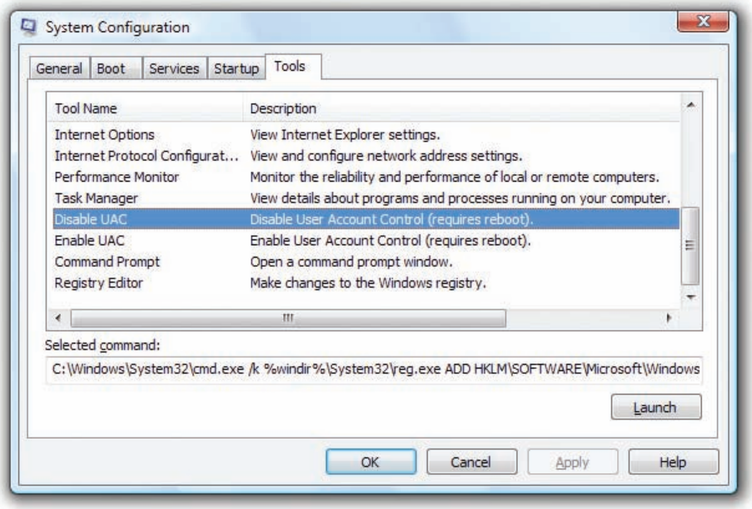
1. In the User Accounts Control Panel applet, you'll see an option to *Turn User Account Control on or off* (see Figure 16.47). Select this option and uncheck the checkbox to turn UAC off. Check the checkbox to turn it on again.
2. Open up the System Configuration utility (msconfig) and select *Disable UAC* on the Tools tab, as shown in Figure 16.48. You'll have to reboot for the changes to take effect. Note you can also turn on UAC from the System Configuration utility.


Control Panel ▸ User Accounts
Search
Tasks
Create a password reset disk
Manage your network passwords
Manage your file encryption certificates
Configure advanced user profile properties
Change my environment variables
See also
Parental Controls
Change your password
Remove your password
Change your picture
Change your account name
Change your account type
Manage another account
Turn User Account Control on or off

Make changes to your user account

dougj
Administrator
Password protected

• **Figure 16.47** Turning User Account Control on or off



Tool Name	Description
Internet Options	View Internet Explorer settings.
Internet Protocol Configurat...	View and configure network address settings.
Performance Monitor	Monitor the reliability and performance of local or remote computers.
Task Manager	View details about programs and processes running on your computer.
Disable UAC	Disable User Account Control (requires reboot).
Enable UAC	Enable User Account Control (requires reboot).
Command Prompt	Open a command prompt window.
Registry Editor	Make changes to the Windows registry.

Selected command:

```
C:\Windows\System32\cmd.exe /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows
```

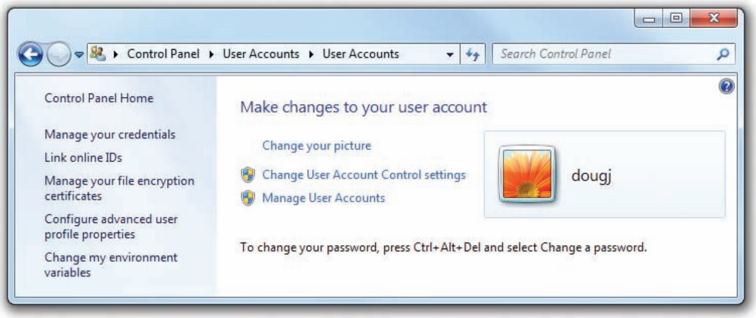
• **Figure 16.48** Disabling UAC in the System Configuration utility

UAC in Windows Vista worked well, but it startled users. Suddenly, users had to deal with UAC, and they didn't like that. Most users simply turned UAC off and added it to the reasons to not like Windows Vista.

All references to Control Panel applets in Windows 7 assume you are using the Small Icon view.

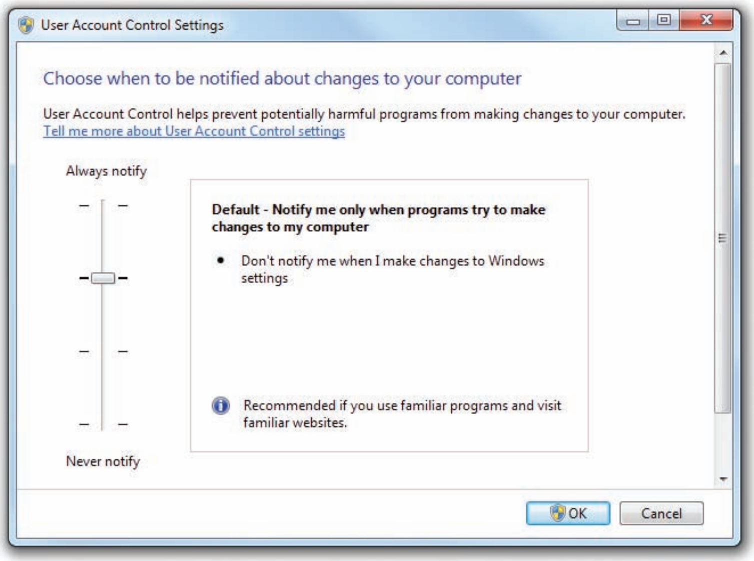
UAC in Windows 7

Microsoft may be a huge company, but it still knows how to react when its customers speak out about features they don't like. Windows 7 unveiled a more refined, less "in-your-face" UAC that makes the feature much easier to use.


Control Panel ▸ User Accounts ▸ User Accounts
Search Control Panel
Control Panel Home
Manage your credentials
Link online IDs
Manage your file encryption certificates
Configure advanced user profile properties
Change my environment variables
Make changes to your user account
Change your picture
Change User Account Control settings
Manage User Accounts
dougj

To change your password, press Ctrl+Alt+Del and select Change a password.

• **Figure 16.49** Change User Account Control settings option



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

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.

• **Figure 16.50** Four levels of UAC

Make sure you know what each of the four UAC levels does.

A More Granular UAC

Microsoft did some research on why UAC drove users nuts, concluding that the problem wasn't UAC itself but the "I'm constantly in your face or you can turn me off and you get no help at all" aspect. To make UAC less aggressive, Microsoft introduced four UAC levels. To see these levels, go to the User Accounts applet and select *Change User Account Control settings*, as shown in Figure 16.49. When you select this option, you see the dialog box in Figure 16-50.

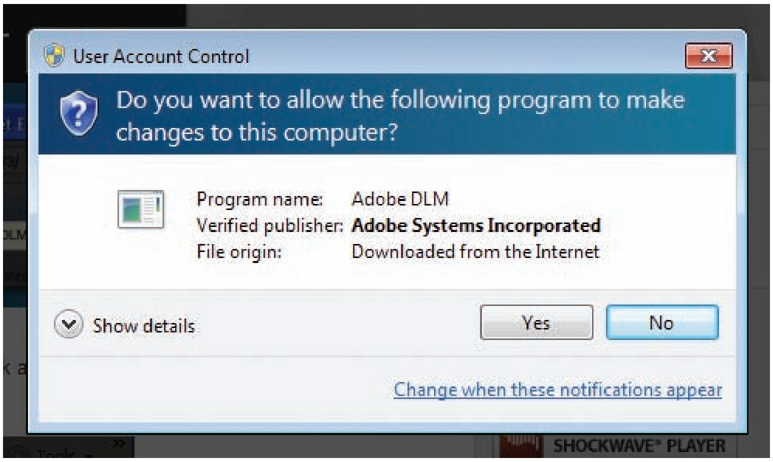
In Figure 16.50, you can see a slider with four levels. The top level (Always notify) means you want UAC to work exactly as it does in Vista, displaying the aggressive consent form every time you do anything that typically requires administrator access. The bottom option (Never notify) turns off UAC. The two levels in the middle are new and are very similar. Both of them do the following:

- Don't notify me when I make changes.
- Notify me only when programs try to makes changes.

The only difference is in *how* they show the change. The second-from-top level will display the typical consent form, but only when programs try to make changes. The third-from-top level displays a consent form, but where the normal consent form dims your desktop and doesn't allow you to do anything but address the form, this consent form just pops up like a normal dialog box.

Program Changes Versus Changes I Make

So what's the difference between a program making a change and you making a change? Take a look at Figure 16.51. In this case, Windows 7 is



User Account Control

Do you want to allow the following program to make changes to this computer?

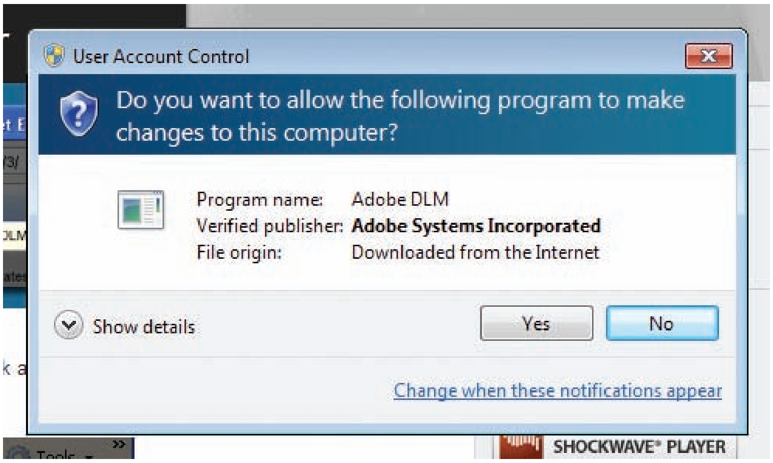
Program name: Adobe DLM
Verified publisher: **Adobe Systems Incorporated**
File origin: Downloaded from the Internet

• **Figure 16.51** Darkened UAC

set to the second-from-top option. A program (the very safe and, judging by the color of the banner, verified) Adobe Download Manager is attempting to install a feature into Internet Explorer. Because this is a program trying to make changes, the UAC consent form appears and darkens the desktop.

The default behavior for UAC in Windows 7 is the second-from-top option, which results in a screen similar to Figure 16.51.

If you lower the UAC to the third-from-top option, you still see a consent form, but now it acts like a typical dialog box, as shown in Figure 16.52.



User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: Adobe DLM
Verified publisher: **Adobe Systems Incorporated**
File origin: Downloaded from the Internet

• **Figure 16.52** Non-darkened UAC

A program such as the Adobe program described earlier is very different from a feature *you* want to change. Notice the shields, as shown earlier in Figure 16.49.

Each of these options isn't a program—each is merely a feature built into Windows. Those shields tell you that clicking the feature next to a shield will require administrator privileges. If you were to pick the Vista-strength UAC option, you'd get a UAC consent prompt when you click one of those features. If you set UAC to any of the three lower settings, however, you'd go straight to that feature without *any* form of UAC consent prompt. Of course, this isn't true if you don't have administrator privileges. If you're a standard user, you'll still be prompted for a password, just as in Vista.

Overall, the improvements to UAC in Windows 7 show that it has a place on everyone's computer. UAC might cause an occasional surprise or irritation, but that one more "Are you sure?" could mean the difference between safe and unsafe computing. So go ahead, turn UAC back on in Windows 7! It's well worth the small inconvenience.

Chapter 16 Review

Chapter Summary

After reading this chapter and completing the exercises, you should understand the following about securing Windows resources.

Create and administer Windows users and groups

- The key to protecting your data is based on two related processes: authentication and authorization. Authentication is the process by which you determine a person at your computer is who he says he is. The most common way to authenticate is by using a user name and password. Once a user is authenticated, he needs authorization, the process that states what a user can and cannot do on that system. Authorization, at least for files and folders, is controlled by the NTFS file system, which assigns permissions to users and groups.
- Passwords are the ultimate key to protecting your computer. If someone learns your user name and password, they can log on to your computer. Protect your passwords. Never give out passwords over the phone. If a user forgets or loses a password, the network administrator should reset the password to a complex combination of letters and numbers. The user should then change the password to something he or she wants, according to the parameters set by the administrator.
- Make sure you use strong passwords: at least eight characters in length, including letters, numbers, and punctuation symbols.
- Windows enables currently logged-on users to create a password reset disk they can use if they forget a password. This is very important to have. If you lose your password and an administrator resets it, you might not have access to all of the files you had access to before, especially if they were encrypted. When you reset a password with a password reset disk, you can log on with the new password and still have access to previously encrypted files. Windows 7 can provide a password hint if you fail to use the proper password on your first attempt to log on.
- A group is a collection of accounts that can define the capabilities of its members. A single account can be a member of multiple groups. Groups are an efficient way of managing multiple users, especially when you are dealing with a whole network of accounts.
- Windows XP Professional provides seven built-in groups: Administrators, Power Users, Users, Backup Operators, Replicator, Everyone, and Guests. These built-in groups have a number of preset capabilities. You cannot delete these groups. Windows XP Home Edition only enables you to use three groups: Administrators, Users, and Guests.
- The professional editions of Windows Vista (Business, Ultimate, and Enterprise) and Windows 7 (Professional, Ultimate, and Enterprise) offer the same groups found in Windows XP Professional and throw in a lot more. Some group types enable people to check on the performance and reliability of a computer but without gaining access to any of the documents on the computer. These groups include Event Log Readers, Performance Log Users, and Performance Monitor Users and provide excellent levels of access for technicians to help keep busy Vista/7 machines healthy.
- Windows XP uses the User Accounts applet in the Control Panel to create and manage user accounts. User Accounts hides the complete list of users, using a simplistic reference to account types that is actually a reference to a user account's group membership. An account that is a member of the local Administrators group is called a computer administrator; an account that belongs only to the Local Users group is called a limited user account.
- Creating users is a straightforward process. You need to provide a user name (a password can and should be added later), and you need to know which type of account to create: computer administrator or limited.
- You can opt out of the Welcome screen and thus require a user to type both a user name and a password. You can also enable or disable Fast User Switching—a feature that enables you to switch to another user account without logging out and thus having to close open programs.
- To add or modify a user account in Windows Vista, you have numerous options depending on which Control Panel view you select and which edition

and update of Vista you have installed. Windows Vista Business and Ultimate, for example, in the default Control Panel Home view, offer the User Accounts applet. Windows Vista Home Premium, in contrast, gives you the User Accounts and Family Safety applet. The Tasks links on the left are similar between editions of Windows, with the addition of Parental Controls in the Home Premium edition, but the main options differ a lot.

- Windows Vista Home Premium uses Vista's version of the Welcome screen for logging on, so each user account has a picture associated with it. You can change the picture from the User Accounts applet. You can also change the name of the user account here and alter the account type.
- With Parental Controls, an administrator account can monitor and limit the activities of any standard user in Windows Vista/7, a feature that gives parents and managers an excellent level of control over the content their children and employees can access. Parental Controls enable you to limit the time that standard users can spend logged on, for example. You can specify acceptable and unacceptable times of day when standard users can log on.
- Creating a user account in Windows 7 is virtually identical to the process in Windows Vista. Windows 7 uses the User Accounts Control Panel applet to manage users.
- The professional editions of Windows enable you to add, remove, and modify users and groups using the advanced Local Users and Groups tool found in the Computer Management console of the Administrative Tools.

Define and use NTFS permissions for authorization

- In Windows, every folder and file on an NTFS partition has a list that contains two sets of data: every user and group that has access to that file or folder, and the level of access each user or group has to that file or folder. A set of detailed and powerful restrictions called NTFS permissions define exactly what any particular account can or cannot do to the file or folder.
- When you create a new file or folder on an NTFS partition, you become the owner of that file or folder, which means you can do anything you want to it, including changing the permissions to prevent anybody, even administrators, from accessing it. The special Take Ownership permission enables an account to seize control of a file or folder. Administrator accounts have Take Ownership permission for everything. Change permission–equipped accounts can give or take away permissions for other accounts.
- In Windows, just about everything in the computer has a Security tab in its Properties dialog box. Every Security tab contains a list of accounts that have permissions for that resource, and the permissions assigned to those accounts. The standard permissions for a folder are Full Control, Modify, Read & Execute, List Folder Contents, Read, and Write. The standard file permissions are Full Control, Modify, Read & Execute, Read, and Write. Permissions are cumulative.
- Moving or copying objects such as files and folders can have an effect on the permissions of those objects, something that techs need to understand. If you copy or move an object from one NTFS partition to another, the new object inherits the permissions associated with the new location. If you copy an object within a partition, the newly created copy inherits the permissions associated with the new location, but the original copy retains its permissions. Any object that you put on a FAT or FAT32 partition loses any permissions because FAT and FAT32 don't support NTFS permissions.

Share a Windows computer securely

- User accounts, groups, and NTFS work together to enable you to share a Windows PC securely with multiple user accounts. You can readily share files, folders, programs, and more. You can share only what should be shared, locking access to files and folders that you want to make private.
- The fact that most users of Windows XP computers will be computer administrators rather than limited users creates a bit of an issue with a computer shared by many users. By default, administrators can see all of the contents of Documents and Settings, where the My Documents folders for each user account reside. Selecting the option to *Make this folder private* in the My Documents Properties dialog box blocks anyone from accessing the contents.
- Use the Shared Documents or Public folders to move files and folders among many users of a single machine. Every account can access the Shared Documents/Public folders and the subfolders within.

- With simple file sharing, you essentially have one local sharing option, and that's to put anything you want to share into the Shared Documents folder or one of its subfolders. To share a folder over a network, you only have a couple of options as well, such as to share or not and, if so, to give full control to everybody. Windows XP Professional enables you to disable simple file sharing and have full control over sharing and permissions.
- Windows Vista enables you to permit specific user accounts to access shared resources and to set the level of access permitted, such as Reader, Contributor, or Co-owner. Vista also uses the Public folder, similar to Shared Documents from Windows XP, which contains multiple shared folders. Any user account can access the Public folder.
- Windows 7 enables you to share libraries using homegroups. Homegroups are secured using a common password.
- You can locate shared folders on your PC using the Shared Folders tool in Administrative Tools.
- Default shares, including all hard drives and the %systemroot% folder, are called administrative shares. They give local administrators access to these resources, whether they log on locally or remotely.
- The scrambling of data through encryption techniques provides the only true way to secure your data from access by any other user. The professional editions of Windows enable a feature called the Encrypting File System (EFS), an encryption scheme that any user can use to encrypt individual files or folders on a computer. The home editions of Windows do not enable encryption.
- Windows Vista/7 Ultimate and Enterprise editions offer full drive encryption through BitLocker Drive Encryption. BitLocker encrypts the whole drive, including every user's files, so it's not dependent on any one account. BitLocker requires a special Trusted Platform Module (TPM) chip on the motherboard to function. The TPM chip validates on boot that the Vista/7 computer hasn't changed and that you still have the same operating system installed.

Secure PCs with User Account Control

- Windows XP made it almost necessary to make your primary account on a computer an administrator account, because limited users can't do common tasks such as installing applications or updating Windows. In Windows Vista, Microsoft rolled out User Account Control to better control access.
- For any action that requires administrator privileges, a dialog box will appear. Standard users need to enter an administer password to continue. Administrators only need to approve the action.
- Windows Vista uses four different UAC prompts: Blocked, Unverified, Verified, and Published by Vista.
- Windows uses small shield icons to warn you if something creates a UAC prompt.
- Windows 7 improved Vista's overactive UAC prompts by establishing four levels of security: Always notify, Notify me only when programs try to make changes to my computer, Notify me only when programs try to make changes to my computer (do not dim my desktop), and Never notify.

Key Terms

administrative shares *(579)*
Administrators group *(558)*
authentication *(555)*
authorization *(555)*
BitLocker Drive Encryption *(580)*
computer administrator *(559)*
Encrypting File System (EFS) *(579)*
encryption *(579)*
Fast User Switching *(562)*
group *(558)*
Guests group *(558)*
inheritance *(572)*
limited user *(559)*
local user account *(555)*
Local Users and Groups *(567)*
NTFS permissions *(569)*
Parental Controls *(565)*
password reset disk *(557)*
permission propagation *(572)*
Power Users group *(558)*

Public folder *(577)*
Shared Documents *(574)*
simple file sharing *(575)*
standard user *(559)*
strong password *(556)*
Take Ownership *(570)*
User Account Control (UAC) *(565)*
User Accounts applet *(559)*
Users group *(558)*
Welcome screen *(561)*

Key Term Quiz

Use the Key Terms list to complete the sentences that follow. Not all terms will be used.

1. The ________________ enables you to manage user accounts in Windows 7.
2. To log on to a standalone Windows PC, you need a(n) ________________.
3. An account that belongs only to the Local Users group in Windows XP is called a(n) ________________.
4. On the ________________, you can click on an icon and type a password to log on to the computer.
5. A(n) ________________ is a collection of user accounts that share the same access capabilities.
6. The ________________ enables standard users to perform common tasks and provides a permissions dialog box when standard users and administrators do certain things that could potentially harm the computer.
7. By default, any file you drop into a folder on an NTFS drive gets the same permissions as those assigned to the folder, a feature called ________________.
8. The ________________ feature of Windows XP Home means you can share or not share a folder. You don't have any finer control than that.
9. Windows Vista has the ________________ available for sharing files and folders with other users of a particular computer.
10. The ________________ enables you to scramble a file or folder and thus hide the contents from anyone, even an administrator.

Multiple-Choice Quiz

1. What process determines the identity of a user?
   A. Authentication
   B. Authorization
   C. Identification
   D. Indemnification
2. Which of the following user account types can create other user accounts?
   A. Administrator
   B. Limited user
   C. Restricted user
   D. Standard user
3. To which of the following groups does a standard user in Windows XP belong by default?
   A. Limited Users
   B. Power Users
   C. Restricted Users
   D. Users
4. Which utility enables you to add users and groups in Windows 7 Professional?
   A. User Account Control
   B. User Accounts applet
   C. Users and Groups applet
   D. Local Users and Groups
5. Which of the following is the strongest password?
   A. 5551212
   B. Spot01
   C. 43*xv
   D. 479love*

6. Which tool would enable a user to recover his encrypted files if he forgets his password?

   A. BitLocker

   B. Encrypting File System

   C. Password reset disk

   D. Password restore disk

7. Which of the following groups can you assign a user to in Windows Vista Home Premium? (Select two.)

   A. Administrators

   B. Power Users

   C. Replicators

   D. Users

8. Which tool in Windows Vista and Windows 7 enables an administrator to create a log that shows all of the applications a user runs or attempts to run?

   A. Create Log

   B. NTFS

   C. Parental Controls

   D. User Account Control

9. Which of the following is *not* a standard NTFS permission?

   A. Copy

   B. Full Control

   C. Modify

   D. Read & Execute

10. As a member of the accounting group, John has Write permission to the Database folder; as a member of the technicians group, John has Read permission to the Database folder. What permission or permissions does John have to the Database folder?

    A. Read only

    B. Write only

    C. Read and Write

    D. Full Control

11. When you copy a file from one folder on the C: drive to another folder on the C: drive, by default what permissions will the copy of that file have if the C: drive is formatted with NTFS?

    A. The copy will retain the permissions the original file has.

    B. The copy will inherit the permissions of the new location.

    C. The copy will lose all permissions.

    D. You can't do that.

12. On a Windows Vista Business computer, where can you place files that other users can access easily?

    A. Public Documents

    B. Public folder

    C. Shared Documents

    D. Shared folder

13. John wants to share a folder in Windows 7 with Liz but wants to make sure she can delete only files she creates in that folder, not the ones he creates. What permission level should he use?

    A. Contributor

    B. Co-owner

    C. Full Control

    D. Reader

14. Which tool in certain Windows Vista and Windows 7 editions enables you to encrypt the contents of a drive, including folders of users other than you?

    A. BitLocker

    B. Drive Encryptor

    C. Encrypting File System

    D. TrueCrypt

15. In Windows 7, how do the two middle levels of UAC security differ?

    A. One creates a prompt for verified programs; the other creates a prompt for unverified programs.

    B. One uses a consent prompt that blocks all other actions; the other uses a consent prompt that does not block other actions.

    C. One creates a prompt that requires a password; the other creates a prompt that does not require a password.

    D. One uses a prompt for standard users only; the other uses a prompt for all users.

Essay Quiz

1. Your boss has tasked you with setting up five Windows 7 workstations, each to be used by three different users. Write a short essay on procedures or policies that should be implemented at each workstation to ensure that each user can share files that need to be shared but can also keep private files that need to be private.
2. Your company has a shared database in Windows Vista. Management must have full access to the database. The salespeople need to be able to access the database and make changes, but can't delete the database. All other employees should be able to read the contents of the database, but not make any changes. Write a short essay describing what groups and permissions you would need to set to make this work.
3. You have a computer with three users, plus an administrator. The three users need to be able to add documents to a folder, but only the administrator should be allowed to see the contents of those documents. Write a short essay describing how you would set up the folder, user accounts, groups, and permissions to make this work.

Lab Projects

• Lab Project 16.1

Take a single computer and create multiple user accounts and groups. Create some shared folders and change permissions on those folders to vary what different user accounts can do. Then experiment. Try to make as many different access types as you can.

• Lab Project 16.2

Experiment with permission propagation. On a computer with two hard drives, both formatted as NTFS, go through the process of copying and moving files and folders—with differing permissions—between folders on a single drive and between the two drives. Note carefully how permissions change or do not change with each step.

• Lab Project 16.3

On a computer with multiple user accounts, experiment with encryption. Encrypt files with one user account and then place those files into shared folders. What happens? Can other accounts access those files? Can they see the filenames? What about the administrator account? Go through the process of taking ownership to see if you can recover the contents of the encrypted files.

• Lab Project 16.4

On a Windows Vista or Windows 7 Ultimate computer, experiment with BitLocker on a second hard drive. Make note of what happens when you remove the drive and put it into another computer. How can you access the data that's been encrypted?