CHAPTER 16

Securing Windows Resources

In this chapter, you will learn how to

- Create and administer Windows users and groups
- Define and utilize NTFS permissions for authorization
- Describe how to share a Windows computer securely

You might ask me, "What's the single greatest aspect that keeps Microsoft Windows the number one operating system in the world?" My answer is "Windows is the easiest operating system for securing resources, individual computers, and entire networks." Windows really gets it right when it comes to protection. Windows uses a combination of user accounts and groups that tie into the NTFS file system to provide incredibly powerful file and folder protection. This user/group/NTFS combo scales down to just a single computer and scales up to a network of computers that can span the world. Windows doesn't just stop at files and folders, either.

The only serious challenge to all this great security is that Windows blurs the line between protecting just a single computer versus protecting a single computer over a network. In this chapter you will see Windows security from the aspect of a single, or *standalone*, machine. In Chapter 26, "Securing Computers," we will revisit most of these security issues and see how the same tools scale up to help you protect a computer in a networked environment.

Essentials

Authentication with 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, so we'll tackle that in the second section of this chapter.

NOTE 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.

Microsoft's answer to the authentication/authorization process is amazing. Inside every Windows computer is a list of names of users who are allowed access to the system. When Windows starts, it presents some form of logon screen where you enter (or select) your user name and then enter something secret (usually a password) that confirms you are the person assigned to that user name. 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 (Figure 16-1).

Each version of Windows has a similar application for creating user accounts. But each one differs enough that it's useful to view them individually. Then we'll look at using passwords and groups to manage users, tasks that all Windows versions share.

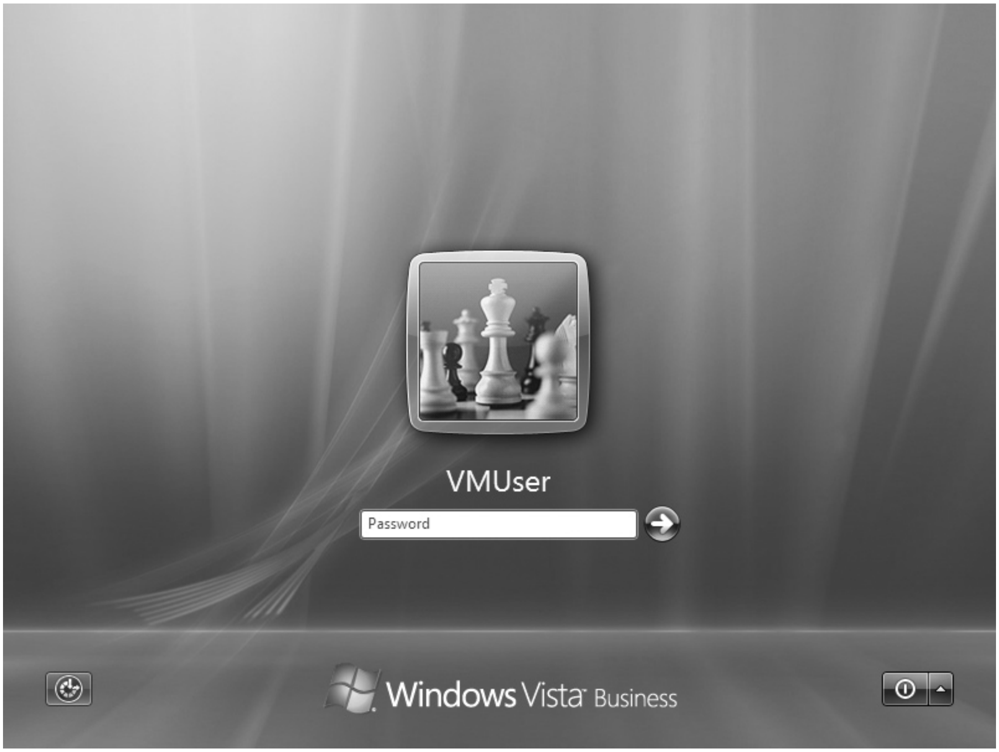


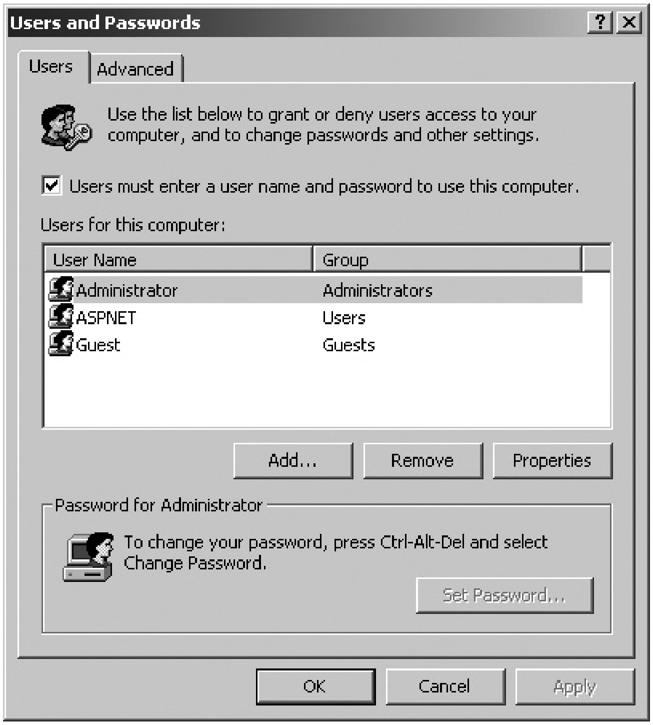
Figure 16-1 Windows Logon screen

Practical Application

Managing Users in Windows 2000

One handy tool for managing users in Windows 2000 is called the *Users and Passwords applet* (Figure 16-2). You access this tool from the Control Panel.

Figure 16-2
Users and Passwords



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

☑ Users must enter a user name and password to use this computer.

Users for this computer:

User Name	Group
Administrator	Administrators
ASPNET	Users
Guest	Guests

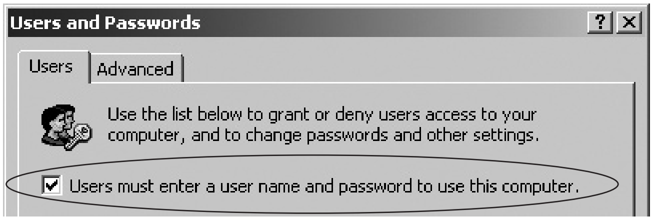
Password for Administrator

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

EXAM TIP Although I've signaled a switch to the Practical Application exam, the competencies on Essentials and Practical Application overlap a lot on the subjects in this chapter. You should know the information here for either exam.

When you install Windows 2000, by default you add two user accounts to the computer: administrator and guest. You can also choose to let the operating system assume that you are the sole user of the computer and not prompt you for a password for logging into Windows. As you might imagine, this severely limits any security on that Windows machine.

You can check this setting after installation by opening the Users and Passwords applet in Control Panel to see the setting for *Users must enter a user name and password to use this computer*. Figure 16-3 shows this choice selected, which means you will see a logon box every time you restart your computer. Also notice that the only user is administrator. That's the account used to log on when no other user is assumed.


Users and Passwords

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

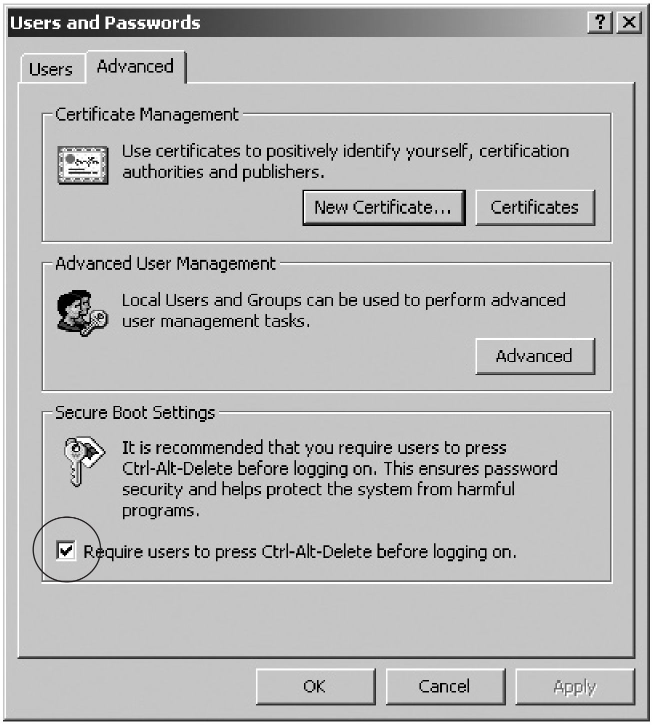
☑ Users must enter a user name and password to use this computer.

Figure 16-3 Security begins with turning on *Users must enter a user name and password to use this computer.*

NOTE When you install Windows, assuming your computer is not made a member of a domain, you may choose to let the OS assume that you are the only user of the computer and do not want to see the logon dialog box.

Using the administrator account is just fine when you're doing administrative tasks such as installing updates, adding printers, adding and removing programs and Windows components, updating device drivers, and creating users and groups. Best practice for the workplace is to create one or more user accounts and only log in with the user accounts, not the administrator account. This gives you a lot more control over who or what happens to the computer.

For the sake of security, a wise administrator also enables the setting on the Advanced tab of Users and Passwords under Secure Boot Settings. If checked, as shown in Figure 16-4, it requires users to press CTRL-ALT-DELETE before logging on. This setting is a defense against


Users and Passwords

Certificate Management

Use certificates to positively identify yourself, certification authorities and publishers.

Advanced User Management

Local Users and Groups can be used to perform advanced user management tasks.

Secure Boot Settings

It is recommended that you require users to press Ctrl-Alt-Delete before logging on. This ensures password security and helps protect the system from harmful programs.

☑ Require users to press Ctrl-Alt-Delete before logging on.

Figure 16-4 Make your computer more secure by enabling Secure Boot Settings.

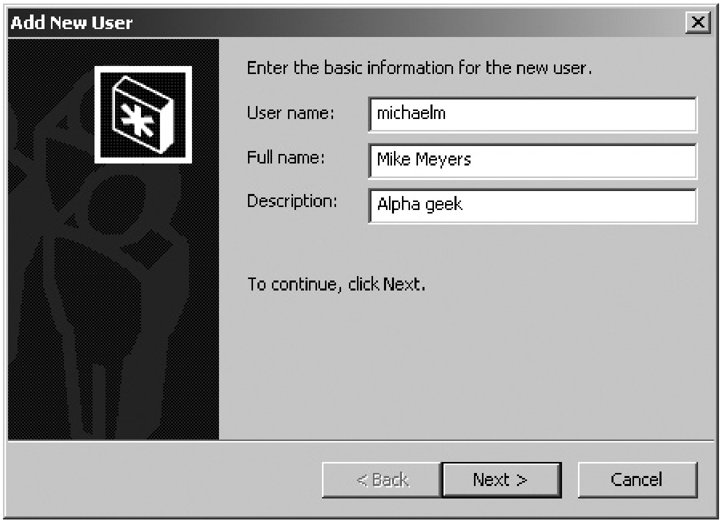
certain viruses that try to capture your user name and password, sometimes by presenting a fake logon prompt. Pressing CTRL-ALT-DELETE removes such programs from memory and allows the actual logon dialog box to appear.

NOTE If the password requirement is turned off and you have user accounts that aren't password protected in Windows 2000 (or other versions of Windows, for that matter), anyone with physical access to your computer can turn it on and use it by pressing the power button. This is potentially a very bad thing!

Creating a new user account enables that user to log on with a user name and password. The administrator can set the rights and permissions for the user and audit the user's access to certain network resources. For that reason, it is good practice to create users on a desktop computer. You are working with the same concepts on a small scale that an administrator must work with in a domain. Let's review the steps in this procedure for Windows 2000.

NOTE To create and manage users, you must be logged on as the administrator, be a member of the Administrators group, or have an administrator account. Assign a password to the administrator account so that only authorized users can access this all-powerful account.

If you're logged on in Windows 2000 as the administrator or a member of the local Administrators group, open the Users and Passwords applet from Control Panel and click the Add button. This opens the Add New User Wizard (Figure 16-5). Enter the user name that the user will use to log on. Enter the user's first and last names in the Full name field, and if you wish, enter some text that describes this person in


Add New User

Enter the basic information for the new user.

User name: michaelm

Full name: Mike Meyers

Description: Alpha geek

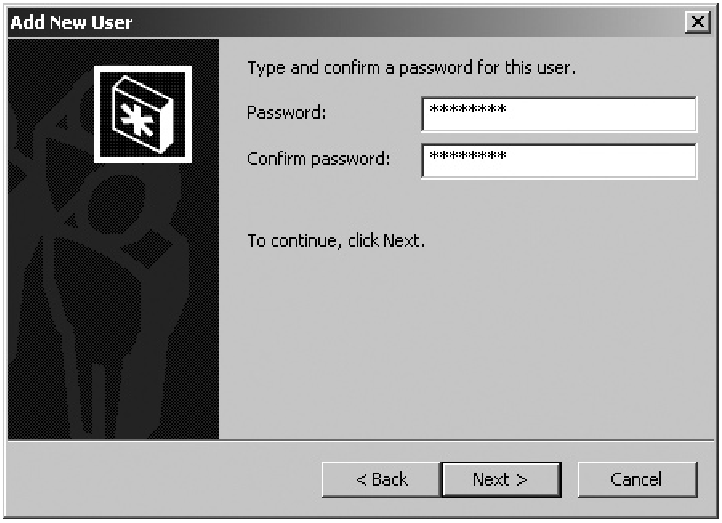
To continue, click Next.

Figure 16-5 Adding a new user

the Description field. If this is at work, enter a job description in this field. The Full name and Description fields are optional.

After entering the user information, click the Next button to continue. This opens a password dialog box where you can enter and confirm the initial password for this new user (Figure 16-6). Click the Next button to continue.

Figure 16-6 Create user password



Add New User

Type and confirm a password for this user.

Password: ********

Confirm password: ********

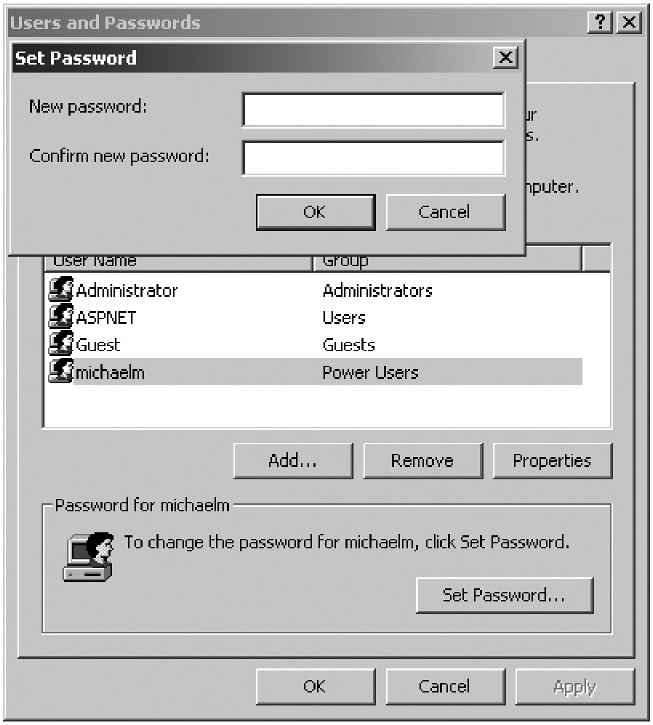
To continue, click Next.

CAUTION Blank passwords or those 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. See the section on passwords later in the chapter.

Now you get to decide what groups the new user should belong to. Select one of the two suggested options—standard user or restricted user—or select the Other option button and choose a group from the drop-down list. Select *Standard User*, which on a Windows 2000 Professional desktop makes this person a member of the local Power Users group as well as the Local Users group. Click the Finish button to close the dialog box. You should see your new user listed in the Users and Passwords dialog box. While you're there, note how easy it is for an administrator to change a user's password. Simply select a user from the list and then click on the Set Password button. Enter and confirm the new password in the Set Password dialog box. Figure 16-7 shows the Set Password dialog box with the Users and Passwords dialog box in the background.

Now let's say you want to change a password. Select the new user in the *Users for this computer* list on the Users page. Then click the Set Password button on the Users page. Enter and confirm the new password and then click the OK button to apply the changes.

Figure 16-7 Set Password dialog box



User Name	Group
Administrator	Administrators
ASPNET	Users
Guest	Guests
michaelm	Power Users

To change the password for michaelm, click Set Password.

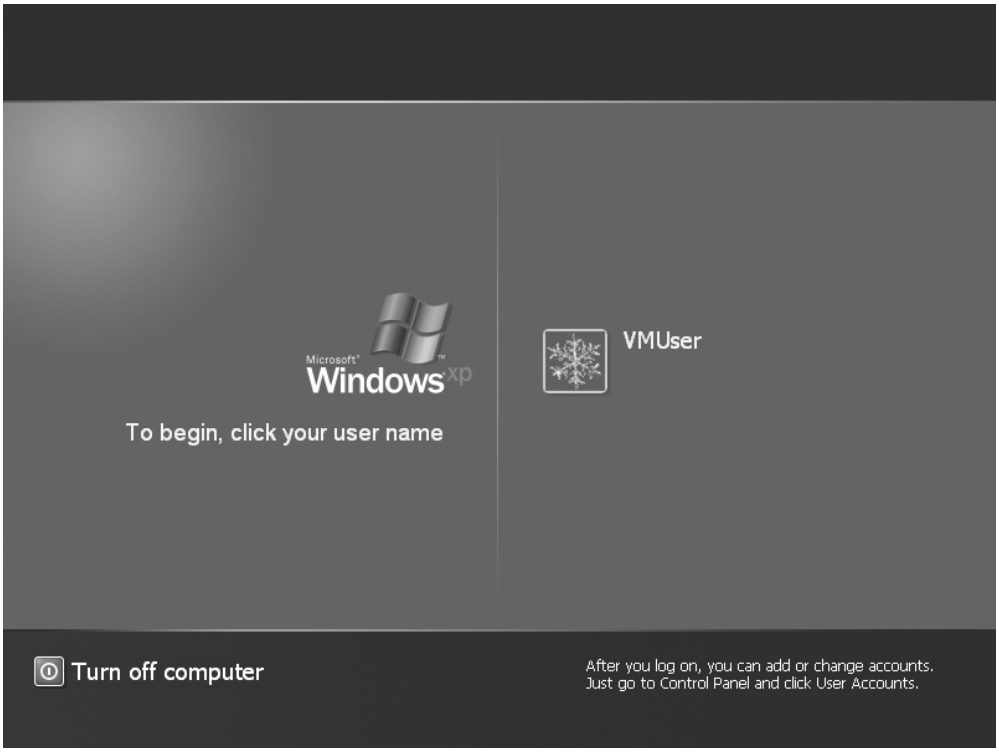
Managing Users in Windows XP

Although Windows XP has essentially the same type of accounts database as Windows 2000, the *User Accounts applet* in the Control Panel replaces the Users and Passwords applet and further simplifies user management tasks.

Windows XP has two very different ways to deal with user accounts and how you log on to a system: the blank user name and password text boxes, reminiscent of Windows 2000, and the Windows XP *Welcome screen* (Figure 16-8). If your Windows XP computer is a member of a Windows domain, your system automatically uses the Windows Classic style, including the requirement to press CTRL-ALT-DEL to get to the user name and password text boxes, just as in Windows 2000. If your Windows XP computer is not a member of a domain, you may use either method, although the Welcome screen is the default. Windows XP Home and Windows XP Media Center cannot join a domain, so these versions of Windows only use the Welcome screen. Windows Tablet PC Edition functions just as Windows XP Professional.

Assuming that your Windows XP system is *not* a member of a domain, I'll concentrate on the XP Welcome screen and some of the options you'll see in the User Accounts Control Panel applet.

The User Accounts applet is very different from the old Users and Passwords applet in Windows 2000. User Accounts hides the complete list of users, using a simplistic



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

Figure 16-8 Windows XP Welcome screen

reference to account types that is actually a reference to its group membership. An account that is a member of the local administrators group is said to be a *computer administrator*; an account that only belongs to the Local Users group is said to be a *limited user* account. Which users the applet displays depends on which type of user is currently logged on (see Figure 16-9). 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 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*

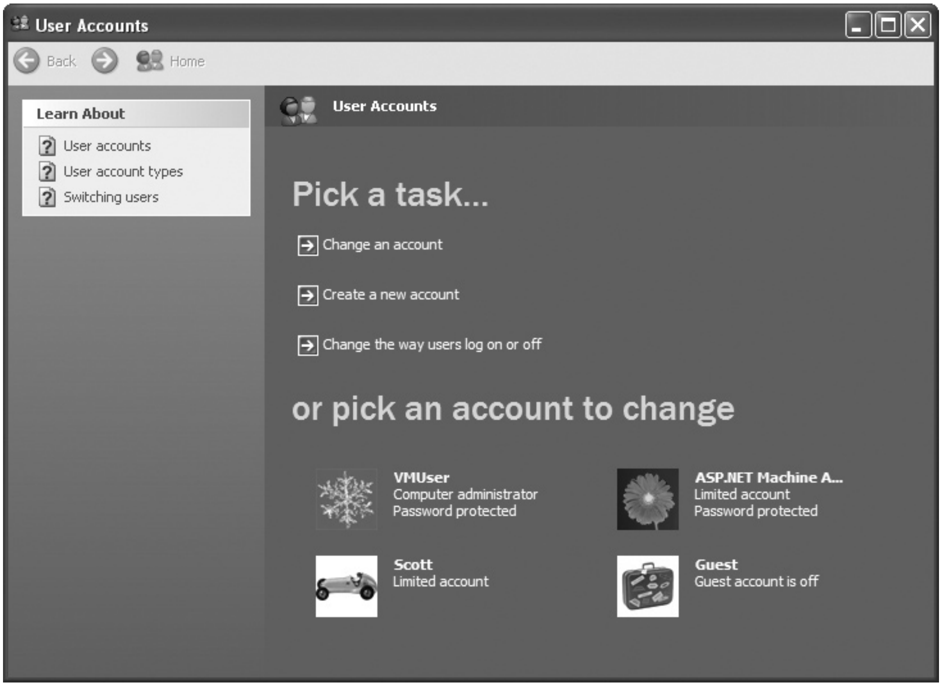


Figure 16-9 User Accounts dialog box showing a computer administrator, a couple of limited accounts, and the guest account (disabled)

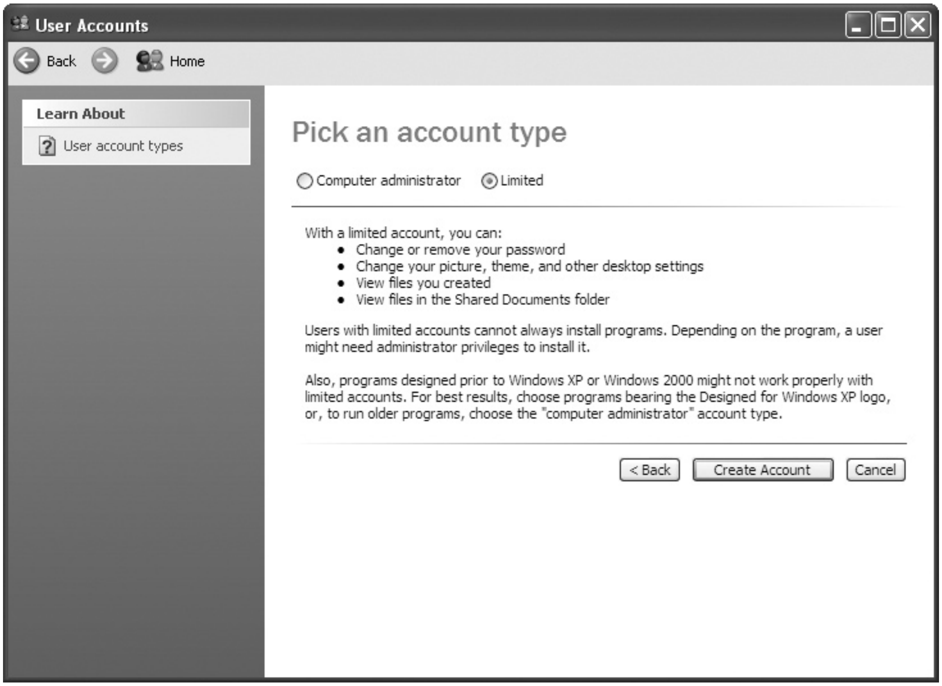
account type page, you can create either type of account (Figure 16-10). Simply follow the prompts on the screen. After you create your local accounts, you'll see them listed when you open the User Accounts applet.

NOTE The old Users and Passwords Control Panel applet is still in every version of Windows XP. If you're on a Windows XP Professional or Windows XP Tablet PC Edition system and your system is part of a domain, the old program comes up automatically when you click the User Accounts applet. If you're running Window XP Professional or Windows XP Tablet PC Edition but *not* on a domain, or if you're running XP Home or Media Center, go to Start | Run and type the following:

```
control userpasswords2
```

This brings up the old applet, which is the best way to change the administrator password on a system.

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 (Figure 16-11). If you select the *Use the*



Pick an account type

○ Computer administrator ● Limited

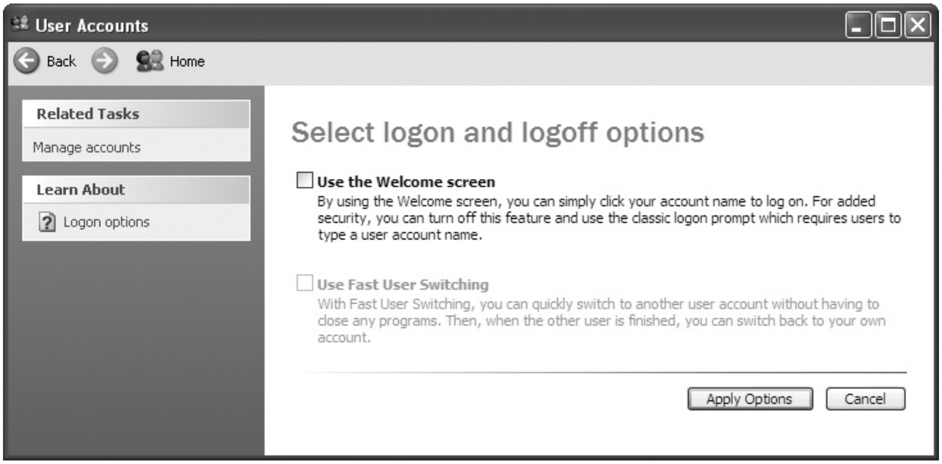
With a limited account, you can:

- 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 16-10 The *Pick an account type* page showing both options available



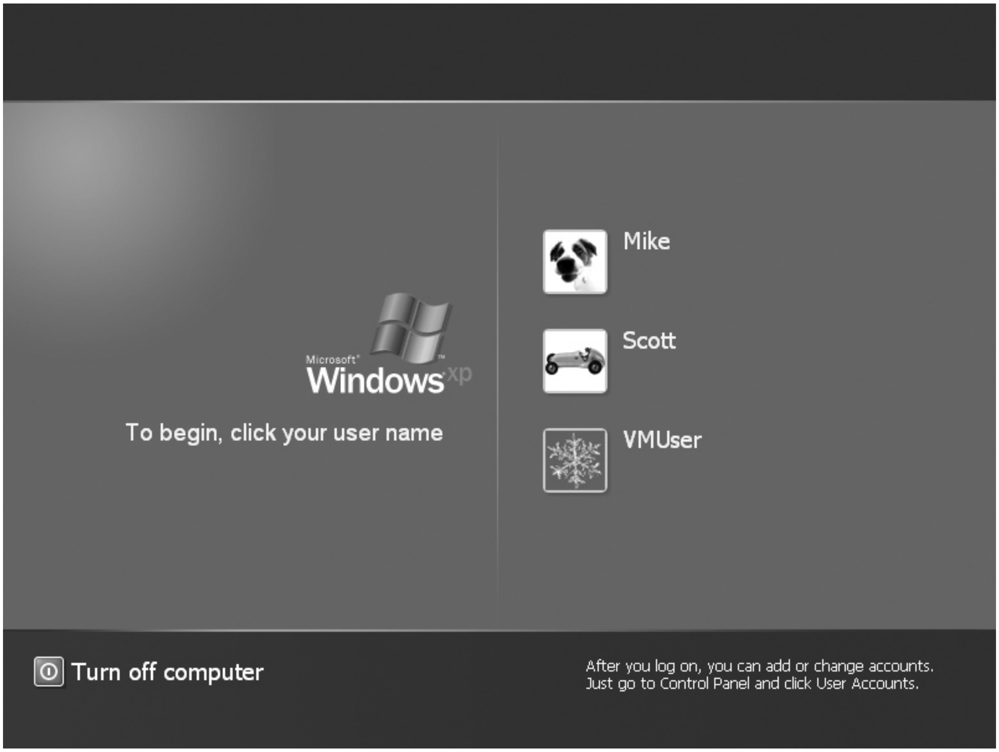
Select logon and logoff options

□ **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 16-11 Select logon and logoff options

Welcome screen checkbox, Windows brings up the friendly Welcome screen shown in Figure 16-12 each time users log in. If this box is unchecked, you'll have to enter a user name and password (Figure 16-13).



Microsoft Windows xp

To begin, click your user name

Mike

Scott

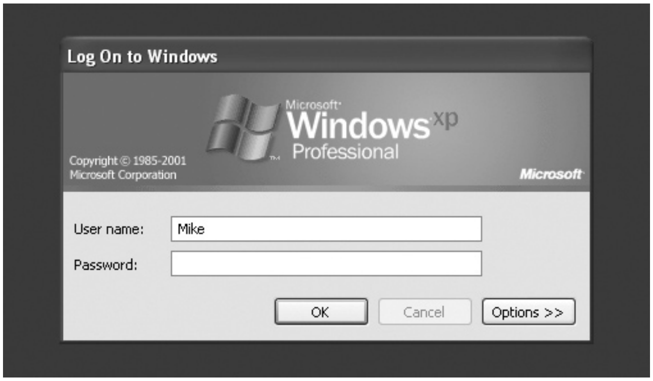
VMUser

Turn off computer

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

Figure 16-12 Single account logon screen

Figure 16-13 Classic Logon screen, XP style



Log On to Windows

Microsoft Windows xp Professional

Copyright © 1985-2001
Microsoft Corporation

Microsoft

User name: Mike

Password:

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 16-14.

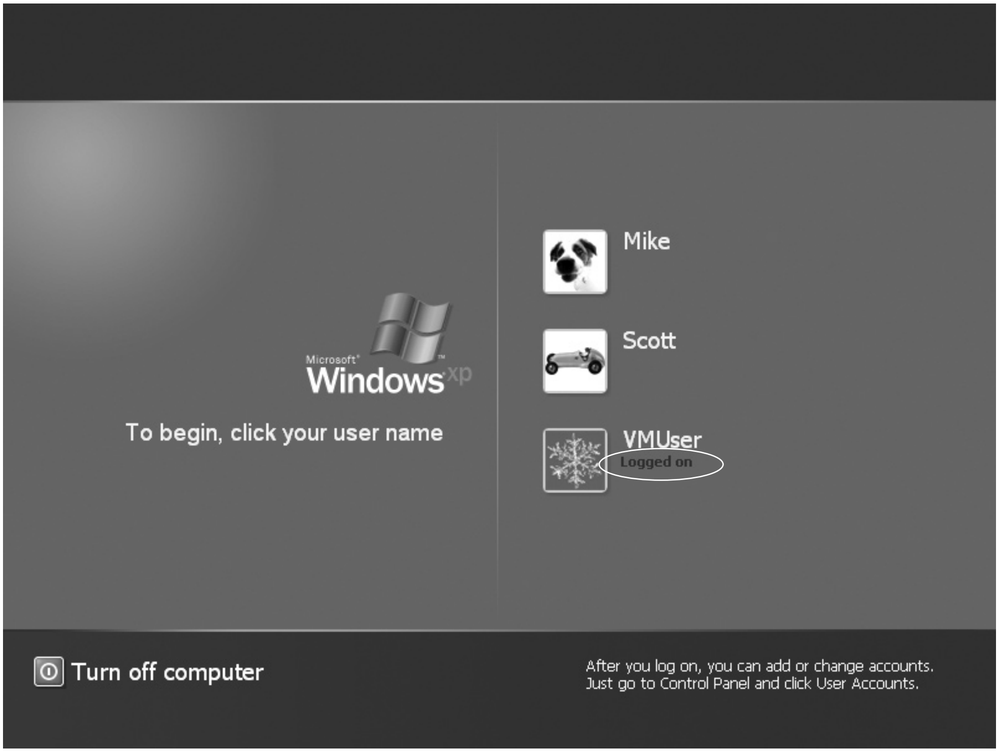

Microsoft Windows xp
To begin, click your user name
Mike
Scott
VMUser
Logged on
Turn off computer
After you log on, you can add or change accounts.
Just go to Control Panel and click User Accounts.

Figure 16-14 Switching Users on the Welcome screen

Managing Users in Windows Vista

Microsoft made some major changes in the transition to Windows Vista, including to the user accounts and the applet used to create and modify them. 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 version 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 (Figure 16-15). Windows Home Premium, in contrast, gives you the User Accounts and Family Safety applet (Figure 16-16). The options under each applet differ as well, as you can see in the screenshots.

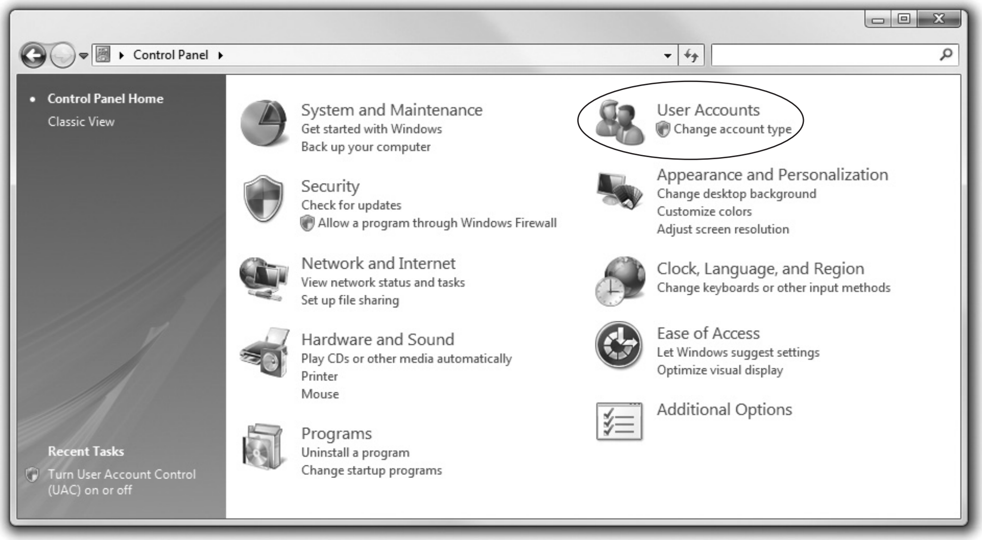


Figure 16-15 User Accounts applet in the Control Panel Home in Windows Vista Ultimate

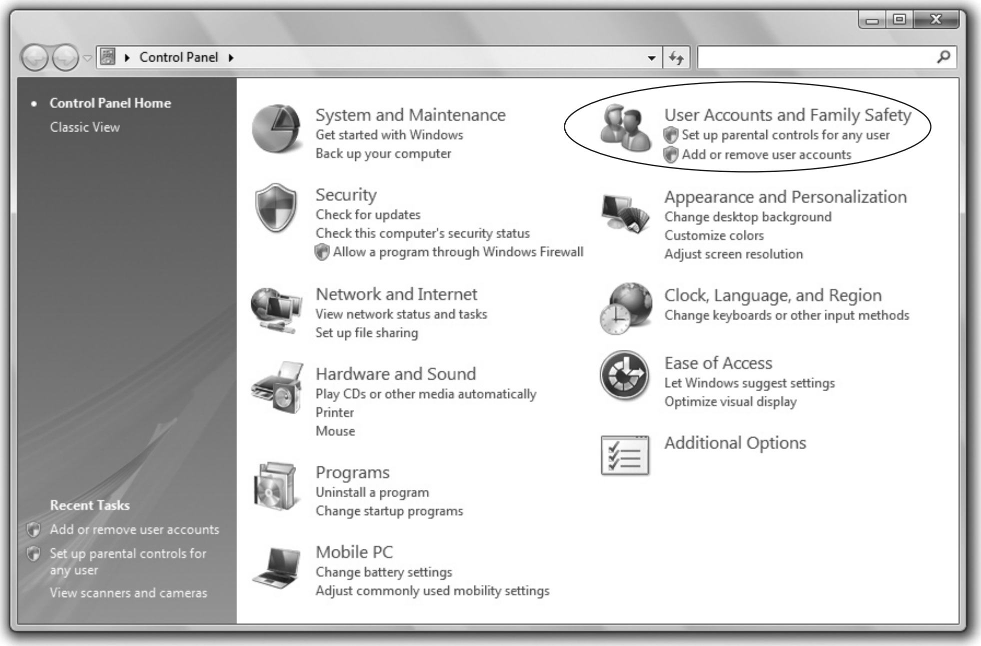
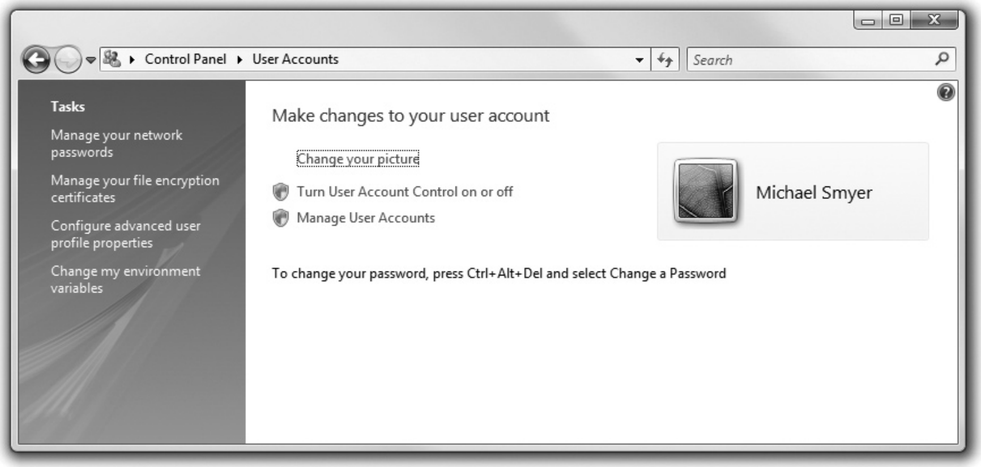

Control Panel
Control Panel Home
Classic View
System and Maintenance
Get started with Windows
Back up your computer
Security
Check for updates
Check this computer's security status
Allow a program through Windows Firewall
Network and Internet
View network status and tasks
Set up file sharing
Hardware 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
Recent Tasks
Add or remove user accounts
Set up parental controls for any user
View scanners and cameras

Figure 16-16 User Accounts and Family Safety applet in the Control Panel Home in Windows Vista Home Premium

Most techs almost immediately change the Control Panel view to Classic, but even there the different versions of Windows—and whether you're logged into a workgroup or a domain—give you different versions of the User Accounts applet. Figure 16-17 shows the User Accounts applet in Windows Vista Business in a domain environment. Figure 16-18 shows the applet in Windows Vista Home Premium.



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

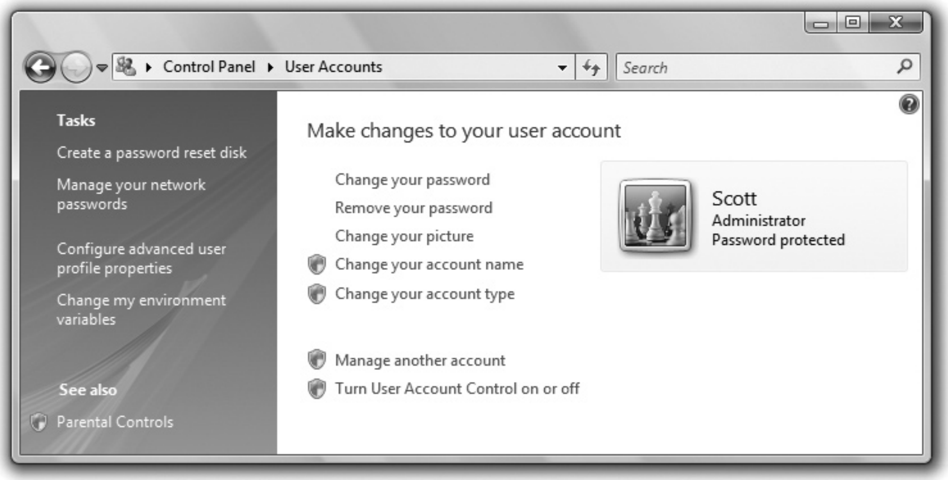
Turn User Account Control on or off

Manage User Accounts

Michael Smyer

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

Figure 16-17 User Accounts applet in Windows Vista Business



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 16-18 User Accounts applet in Windows Vista Home Premium

The Tasks options on the left are similar, with the addition of Parental Controls in the Home Premium edition, but the main options differ a lot. This chapter assumes a standalone machine, so we'll look more closely at the options with Vista Home Premium.

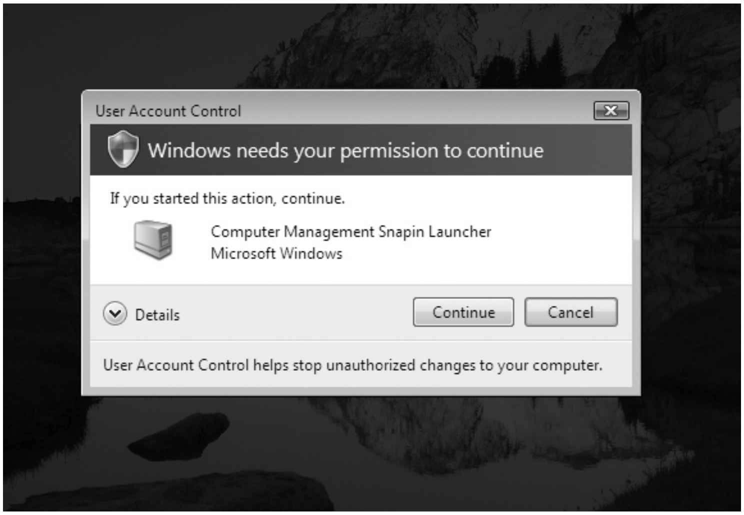
Windows Vista Home Premium uses Vista's version of the Welcome screen for logging in, so each user account has a picture associated with it. You can change the picture from the User Accounts applet. You can also change the name of the user account here and alter the account type, demoting an account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

NOTE You have to have one account as an administrator. 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 in. Because such accounts have full control over the computer, malware that slipped in with that 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 (Figure 16-19) when standard users *and* administrators do certain things that could potentially harm the computer (such as attempt to install a program). Vista user accounts now function much more like user accounts in Linux and Macintosh OS X, with programs asking for administrative permission before making changes to the computer.


User Account Control

Windows needs your permission to continue

If you started this action, continue.

Computer Management Snapin Launcher
Microsoft Windows

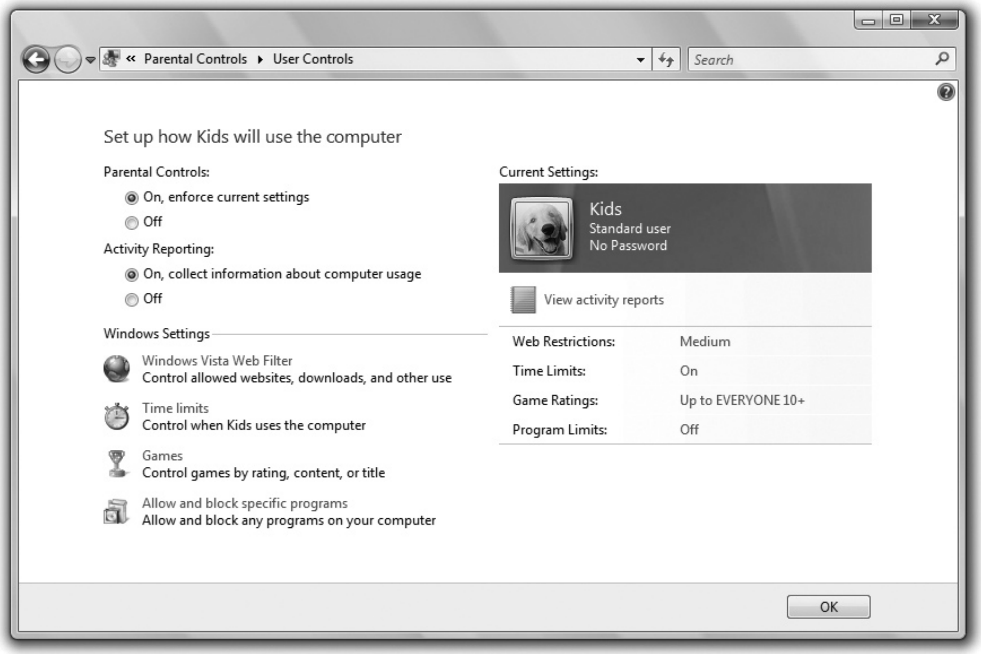
User Account Control helps stop unauthorized changes to your computer.

Figure 16-19 Prompting for permission

NOTE When Windows Vista debuted, most users and techs hated the User Account Control. The dialog box came up seemingly whenever you tried to do anything, prompting for a password if you were logged in as a Standard User or for confirmation if logged in as an administrator. Turning off the UAC prompt—though definitely not recommended by Microsoft—is readily accomplished in the User Accounts applet in the Control Panel. Click the link to *Turn User Account Control on or off* and deselect the checkbox next to Use User Account Control (UAC) to help protect your computer.

Parental Controls

With *Parental Controls*, you can monitor and limit the activities of any Standard User in Windows Vista, a feature that gives parents and managers an excellent level of control over the content their children and employees can access (Figure 16-20). 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.



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 16-20 Parental Controls

Parental Controls enable you to limit the time that standard users can spend logged in. You can specify acceptable and unacceptable times of day when standard users can log in. 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+.

Managing Users in General

Aside from the specific aspects of managing users in each particular version of Windows, there are a few security considerations that apply to every version of Windows, such as using appropriate passwords and creating user groups.

Passwords

Passwords are the ultimate key to protecting your computers. A user account with a valid password gets you into any system. Even if the user account only has limited permissions, you still have a security breach. Remember: for a hacker, just getting into the network is half the battle.

Protect your passwords. Never give out passwords over the phone. If a user forgets a password, an administrator should reset the password to a complex combination of letters and numbers, and then allow the user to change the password to something the user 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.

NOTE 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 combinations of common words and numbers to try to hack a password.

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

Once you've forced your users to choose strong passwords, you should make them change passwords at regular intervals. Although this concept sounds good on paper, in the real world it is a hard policy to maintain. 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!

NOTE 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 26, "Securing Computers," goes into detail about setting up Local Policies and Group Policy.

Windows XP and Windows Vista enable 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 an administrator resets the password by using User Accounts or Local Users and Groups, and you then log on with the new password, you will discover that you cannot access some items, including files you encrypted when logged on with the forgotten password. 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.

NOTE See the last section of this chapter, "Protecting Data with Encryption," for the scoop on the ultimate in security.

Best of all, with the password reset disk, users have the power 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! If you need to create a password reset disk for a computer on a network (domain), search the Help system for "password reset disk" and follow the instructions for password reset disks for a computer on a domain.

Windows Vista has an obvious option in the Tasks list to *Create a password reset disk*. You'll need to have a floppy disk inserted or a USB flash drive to create the disk.

Groups

A *group* is simply a collection of accounts that share the same access capabilities. A single account can be a member of multiple groups. Groups are essential for managing a network of computers but also can come in handy on a single computer with multiple users.

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. For example, you can make a group called Accounting and put all of 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, you just add the new 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.

Groups in Windows 2000 Windows 2000 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.

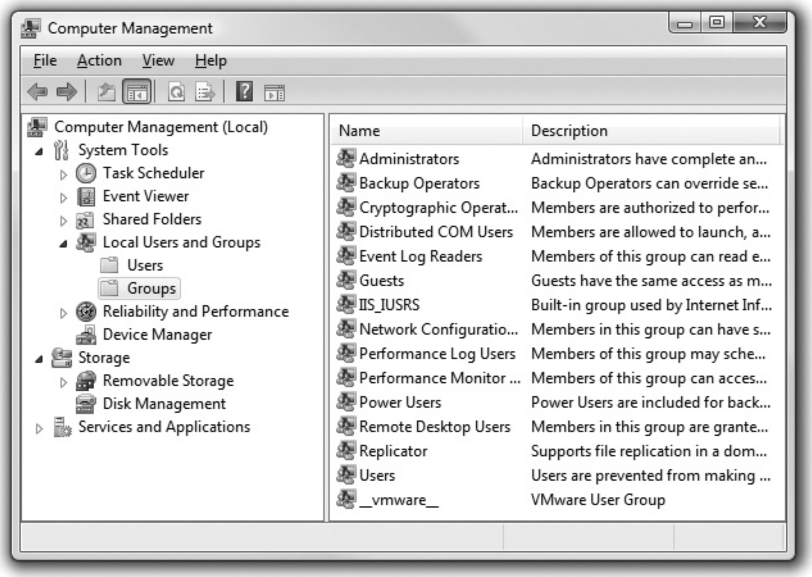
- **Administrators** Any account that is a member of the *Administrators group* has complete administrator privileges. It is common for the primary user of a Windows system to have her account in the Administrators group.
- **Power Users** Members of the *Power Users group* are almost as powerful as 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.
- **Backup Operators** Backup operators have the same rights as users, except that they can run backup programs that access any file or folder—for backup purposes only.
- **Replicator** Members of the Replicator group can replicate files and folders in a domain.
- **Everyone** This group applies to any user who can log on to the system. You cannot edit this group.
- **Guests** Enabling the *Guests group* lets 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 for every version of Windows.

Groups in Windows XP Windows XP diverges a lot from Windows 2000 on user accounts. If you're running XP Professional and you are on a Windows domain, XP offers all of the accounts listed previously, but it adds other specialized groups, including HelpServicesGroup and Remote Desktop Users. Windows XP Home and XP Professional, when installed as a standalone PC or connected to a workgroup but not a domain, run in a specialized networking mode called *simple file sharing*. A Windows XP system running simple file sharing has only three account types: computer administrator, limited user, and guest. Computer administrators can do anything, as you might suspect. Limited users can access only certain things and have limits on where they can save files on the PC. The guest account is disabled by default but works the same way as in Windows 2000.

Groups in Windows Vista The professional editions of Windows Vista (Business, 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 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. These groups provide excellent levels of access for technicians to help keep busy Vista machines healthy.

Like Windows XP, the home editions of Windows Vista (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.

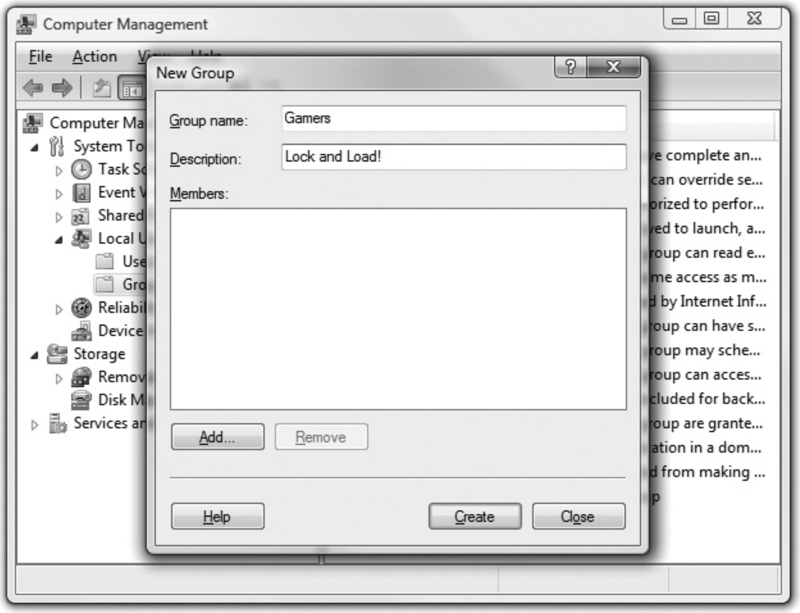
Adding Groups and Changing Group Membership The professional versions of Windows—including Windows 2000, XP, and Vista—enable you to add new groups to your computer by using the *Local Users and Groups* tool, found in the Computer Management applet of the Administrative Tools. This tool also enables you to create user accounts and change group membership for users. Figure 16-21 shows the Local Users and Groups in Windows Vista with the 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 16-21 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 (Figure 16-22).

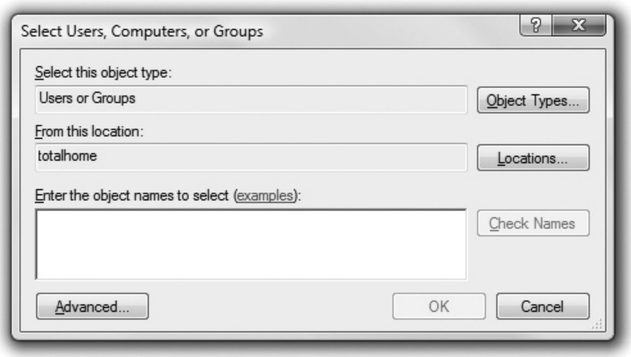


Group name: Gamers

Description: Lock and Load!

Figure 16-22 New Group dialog box in Windows Vista

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. In Vista it's called the Select Users, Computers, or Groups dialog box (Figure 16-23). The Windows 2000 dialog box presents a list of user accounts. Windows XP and Vista add some complexity to the tool.



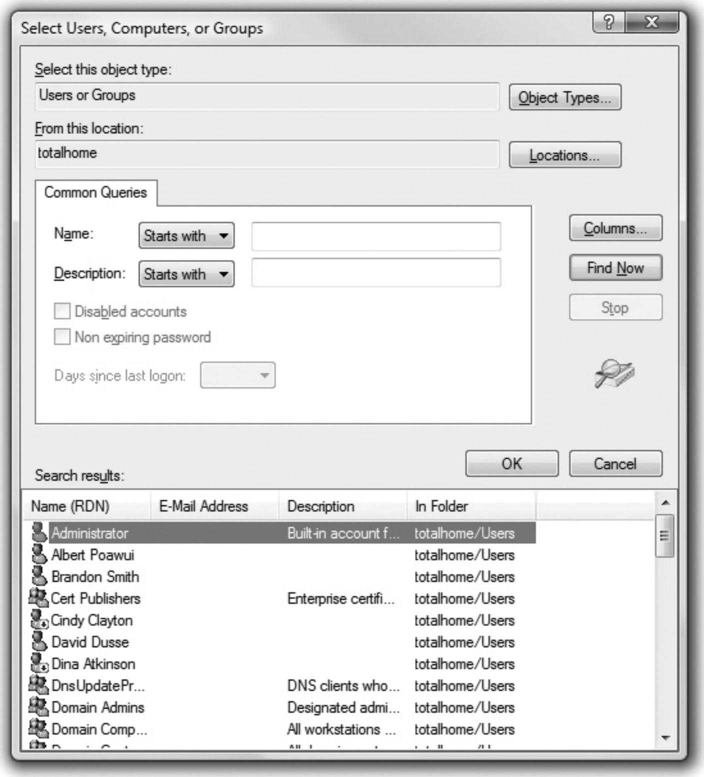
Select this object type: Users or Groups

From this location: totalhome

Enter the object names to select (examples):

Figure 16-23 Select Users, Computers, or Groups dialog box

A user account, a group, a computer; these are all object types in Microsoft lingo. To give you a lot of control over what you do or how you select various objects, Microsoft beefed up this dialog box. The short story of how to select a user account is to click the Advanced button to expand the dialog box and then click the Find Now button (Figure 16-24).



Select Users, Computers, or Groups

Select this object type: Users or Groups

From this location: totalhome

Common Queries

Name: Starts with

Description: Starts with

□ Disabled accounts

□ Non expiring password

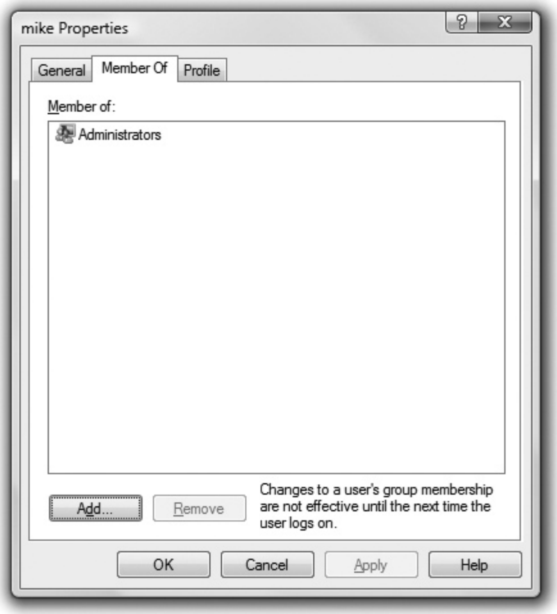
Days since last logon:

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 16-24 Select Users, Computers, or Groups dialog box with Advanced options expanded to show user accounts

You can add or remove user accounts from groups with the Local Users and Groups tool. You 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 (Figure 16-25). Click Add to add group membership. Select a group and click Remove to take away a group membership. It's a clean, well-designed tool.



Member of:

Administrators

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

Figure 16-25 Properties dialog box of a user account, where you can change group memberships for that account

Authorization through NTFS

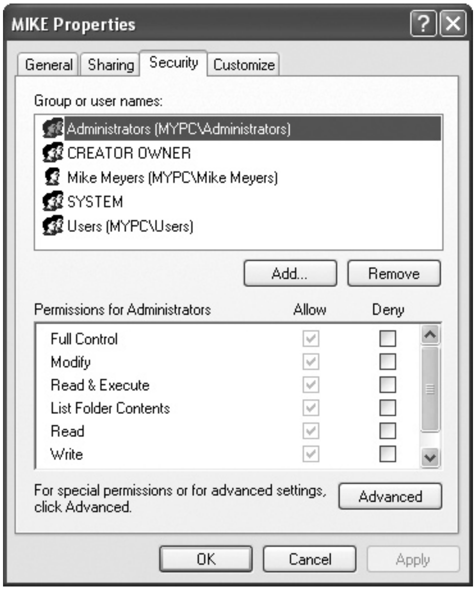
User accounts and passwords provide the foundation for securing a Windows computer, enabling users to authenticate onto that PC. The essential next step in security is authorization, determining what a legitimate user can do with the resources—files, folders, applications, and so on—on that computer. Windows uses the NT file system and permissions to protect its resources.

NTFS Permissions

In Windows 2000, XP, Vista, and 7, 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 a 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 let someone create a folder and not allow other people to make subfolders. NTFS file and folder permissions are so complicated that entire books have been written on them! Fortunately, the CompTIA A+ certification exams test your understanding of only a few basic concepts of NTFS permissions: Ownership, Take Ownership permission, Change permissions, 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. A newly created file or folder by default gives everyone full permission to access, delete, and otherwise manipulate 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 in my Windows XP 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 16-26).
- **File permissions** File permissions are similar to Folder permissions. We'll talk about File permissions right after we cover Folder permissions.



Group or user names:

Administrators (MYPC\Administrators)
CREATOR OWNER
Mike Meyers (MYPC\Mike Meyers)
SYSTEM
Users (MYPC\Users)

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

For special permissions or for advanced settings, click Advanced.

Figure 16-26 The Security tab lets you set permissions.

In Windows, just about everything in the computer has a Security tab in its properties, 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.
- **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 read any file in the folder.
- **Write** Enables you to write to files and create new files and folders.

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** If the file is a program, you can run it.
- **Read** If the file is data, you can read it.
- **Write** Enables you to 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 as well as the Write permission.

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.

NOTE Windows versions 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 the properties and see a Security tab as you can in the professional-oriented versions of Windows. Windows Home versions 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."

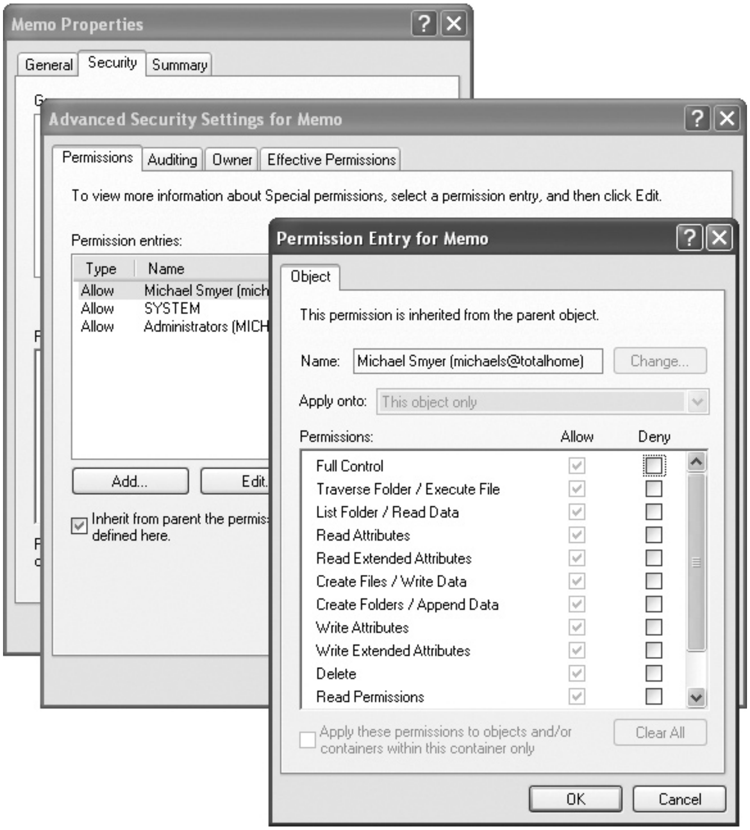
If you look at the bottom of the Security tab in Windows 2000, you'll see a little check box that says Allow Inheritable Permissions from Parent to Propagate to This Object. In other words, any files or subfolders created in this folder get the same permissions for the same users/groups that the folder has, a feature called *inheritance*. Deselecting this option enables you to stop users from getting a specific permission via inheritance. Windows XP and Windows Vista have the same feature, only it's accessed through the Advanced button in the Security tab. Windows also provides explicit Deny functions for each option (Figure 16-27). Deny overrules inheritance.

EXAM TIP 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.

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. So 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. So the new copy can have different permissions than the original.

Figure 16-27 Special permissions



To view more information about Special permissions, select a permission entry, and then click Edit.

Permission entries:

Type	Name
Allow	Michael Smyer (mich
Allow	SYSTEM
Allow	Administrators (MICH

☑ Inherit from parent the permis defined here.

This permission is inherited from the parent object.

Name: Michael Smyer (michaels@totalhome)

Apply onto: This object only

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	☑	□
Write Extended Attributes	☑	□
Delete	☑	□
Read Permissions	☑	□

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

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. So 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 simply 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 giving out administrative permissions (for obvious reasons). If one 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 tape 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 2000, Windows XP, and Windows Vista separately and then finish with a look at a few other sharing and security issues involving sharing.

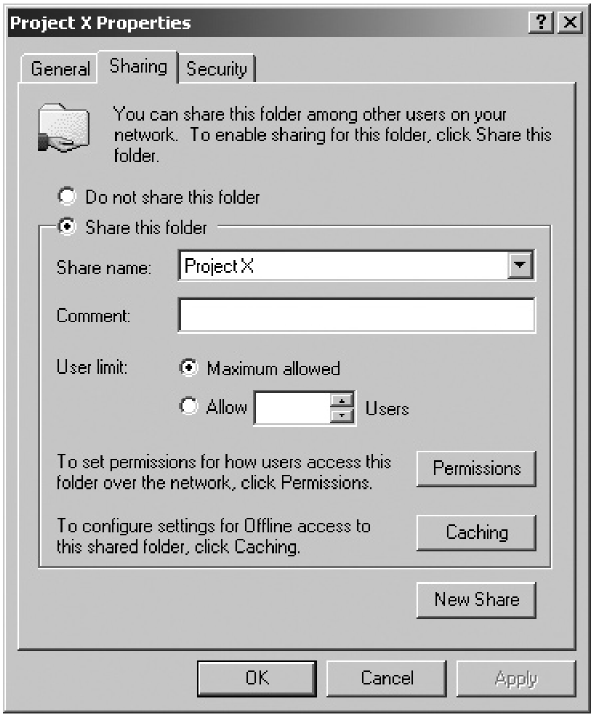
Sharing in Windows 2000

Every user account on a Windows 2000 computer gets a My Documents folder, the default storage area for personal documents. That sounds great, but every account that's a member of the Administrators group can view the contents of everybody's My Documents folder, by default.

A typical way to create a secure shared Windows 2000 computer is to change the permissions on your My Documents folder to give yourself full control, but take away the permissions that allow other accounts access. You also should not create user accounts that go beyond Power Users or even Standard Users.

Finally, make a folder for people to share so that moving files to and from accounts is easy. A typical example would be to create a folder on the C: drive called Shared and then alter the permissions, giving full control to everyone.

To make changes to the permissions on folders, right-click and select Sharing to open the Properties dialog box with the Sharing tab already selected (Figure 16-28). Click the Share this folder check box and change the options to what you want.



You can share this folder among 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: Project X

Comment:

User limit: ● Maximum allowed

○ Allow Users

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

To configure settings for Offline access to this shared folder, click Caching.

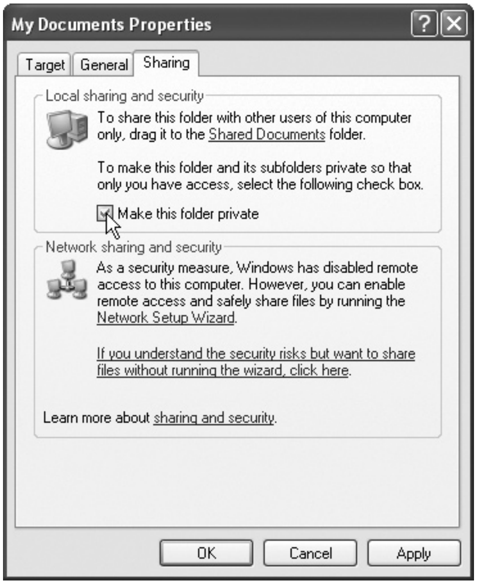
Figure 16-28 Sharing tab on Properties for the Shared folder

Sharing in Windows XP

Microsoft tried to make Windows XP more shareable securely than previous versions of Windows. To this end, they included several features. First, just as with Windows 2000, each user account gets a series of folders in My Documents that the user can share and administrators can access. But Windows XP also comes with a set of pre-made folders called *Shared Documents* 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 (Figure 16-29).



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.

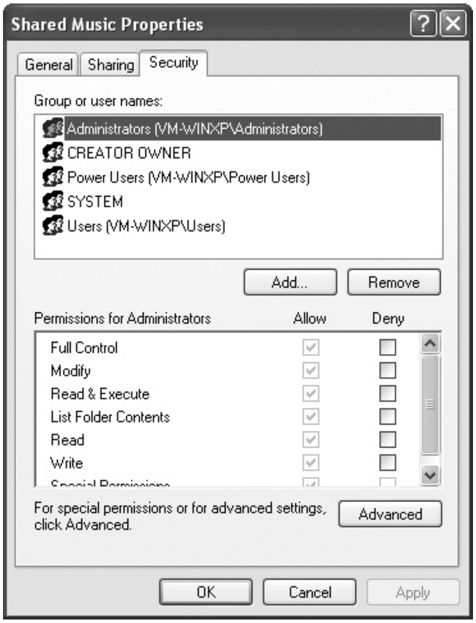
Learn more about sharing and security.

Figure 16-29 Making personal documents secure from prying eyes

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 check box 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.

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 and the sub-folders within, such as Shared Music and Shared Pictures (Figure 16-30). Because new folders inherit the permissions of parent folders, by default any new subfolder you create in Shared Folders can be accessed by any account.



Shared Music Properties

Group or user names:

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

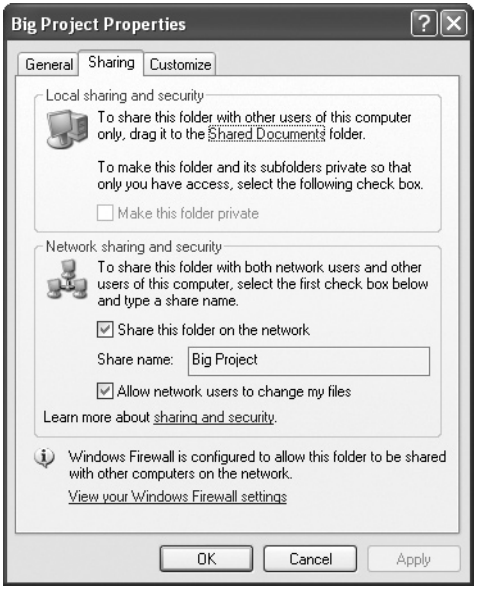
Permissions for Administrators	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□
Special Permissions	☑	□

For special permissions or for advanced settings, click Advanced.

Figure 16-30 Shared Music Properties dialog box

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. 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 16-31. It's pretty much all or nothing.



Big Project Properties

Local sharing and security

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

Network sharing and security

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 16-31 Folder shared, but seriously not secure

Windows XP Home and Media Center only give you the simple file sharing, 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, in some form of Windows Explorer, such as My Documents, go to 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 16-32, and then click OK.

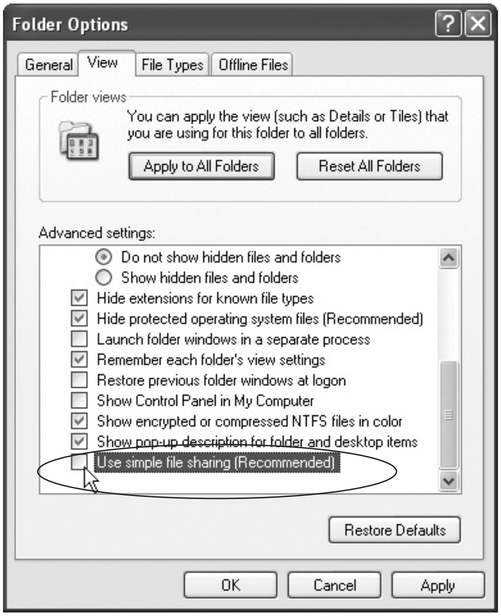


Figure 16-32 Windows Logon screen

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

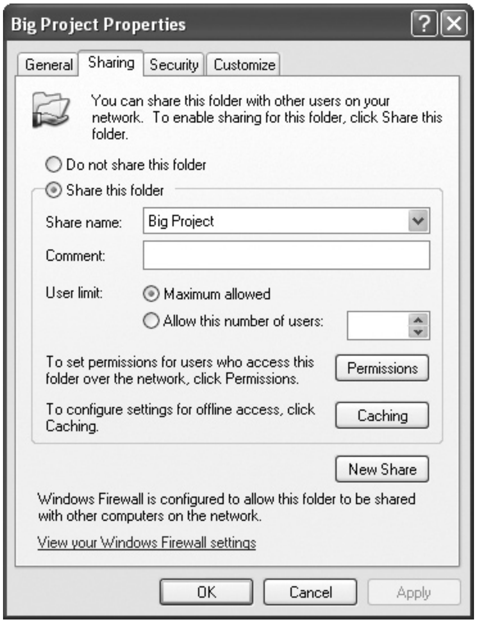
OK | Cancel | Apply

When you access sharing and security now, you'll see a more fully formed security dialog box reminiscent of the one you saw with Windows 2000 (Figure 16-33).

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

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; for example, enabling you to target shared files and folders to specific user accounts. They 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 into the Public folder.



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.

To configure settings for offline access, click Caching.

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

Figure 16-33 Full sharing and security options in Windows XP

Targeted Sharing

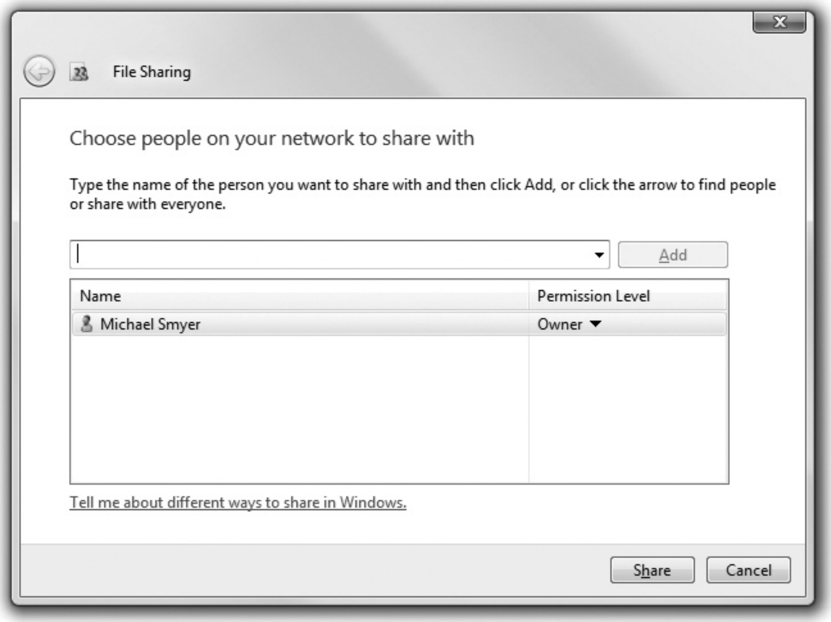
To share a folder or file with specific users—or to everyone, for that matter—you simply right-click on it and select Share. This opens the File Sharing dialog box where you can select specific user accounts from a drop-down list (Figure 16-34).

NOTE 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.

Once you select a user account, you can then choose what permission level to give that user. You have three choices: Reader, Contributor, or Co-owner (Figure 16-35). *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.) A *co-owner* can do anything.

Public Folder

The *Public folder* offers 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 in the Public folder or one of the many subfolders, such as Public Documents or Public Pictures (Figure 16-36). Note that the Public folder does not give you any control over what someone accessing the files contained within can do with those files.



File Sharing

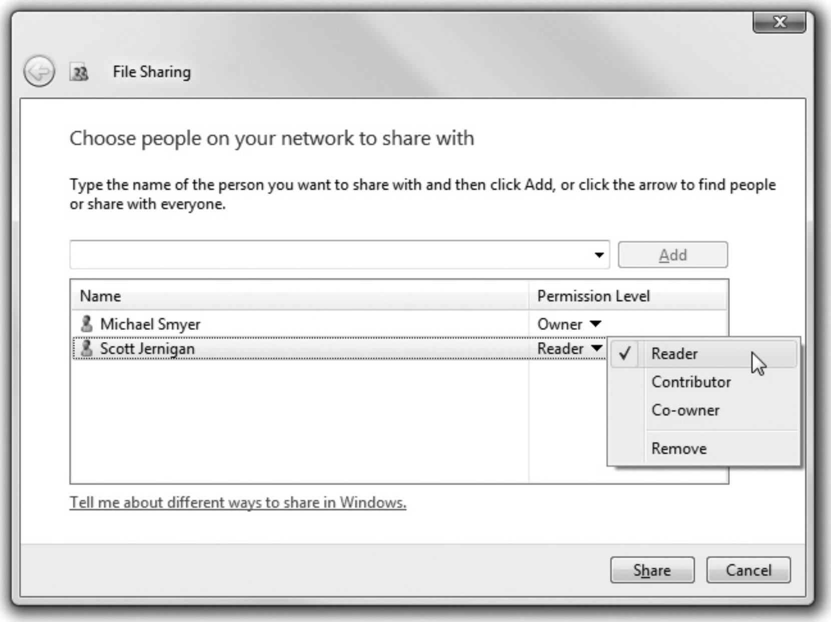
Choose people on your network to share with

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

Tell me about different ways to share in Windows.

Figure 16-34 File Sharing dialog box on a standalone machine



File Sharing

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

Tell me about different ways to share in Windows.

Figure 16-35 Permissions options

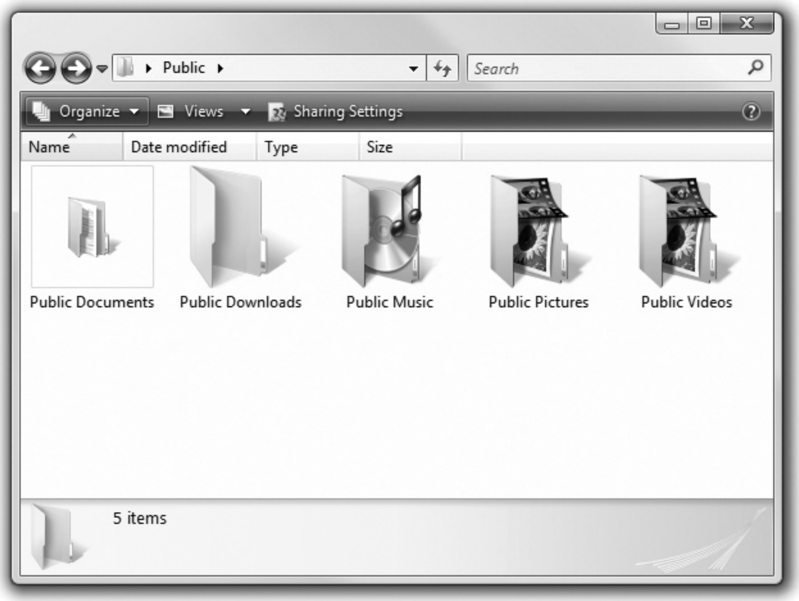


Figure 16-36 Shared folders in the Public folder

Locating Shared Folders

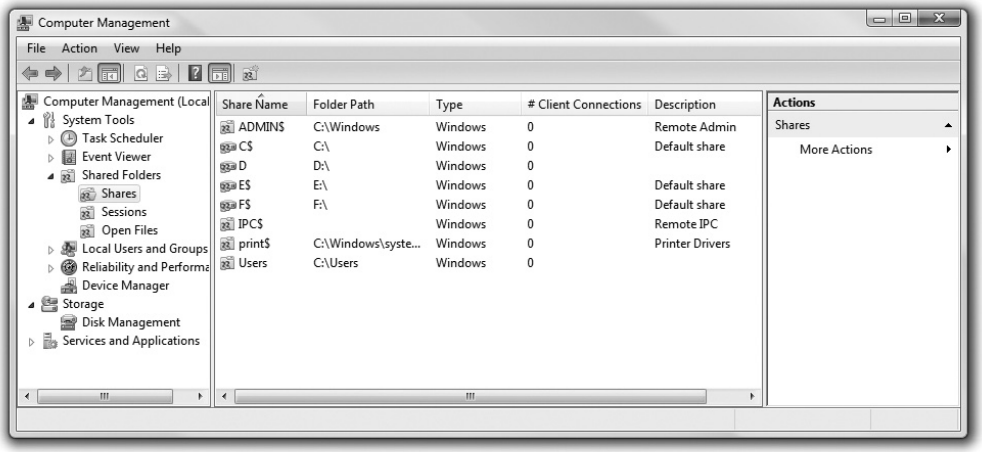
Before you walk away from a computer, you should check for any unnecessary or unknown (to you) shared folders on the hard drives. This enables you to make the computer as secure as possible for the user. When you open My Computer or Computer, shared folders don't just jump out at you, especially if they're 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, 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 (Figure 16-37).

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.

Administrative Shares

A close glance at the screenshot in Figure 16-37 might have left some of you with raised eyebrows and quizzical looks. What kind of share is ADMIN$ or F$?



Share Name	Folder Path	Type	# Client Connections	Description
ADMIN$	C:\Windows	Windows	0	Remote Admin
C$	C:\	Windows	0	Default share
D	D:\	Windows	0	
E$	E:\	Windows	0	Default share
F$	F:\	Windows	0	Default share
IPC$		Windows	0	Remote IPC
print$	C:\Windows\syste...	Windows	0	Printer Drivers
Users	C:\Users	Windows	0	

Figure 16-37 Shared Folders tool in Computer Management

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 or C:\WINNT—and a couple of others, depending on the system. These *administrative shares* give local administrators administrative access to these resources, whether they log in 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.

NOTE 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 into a computer remotely as administrator with no password, you get guest access rather than administrator access. That neatly nips potential exploits in the bud.

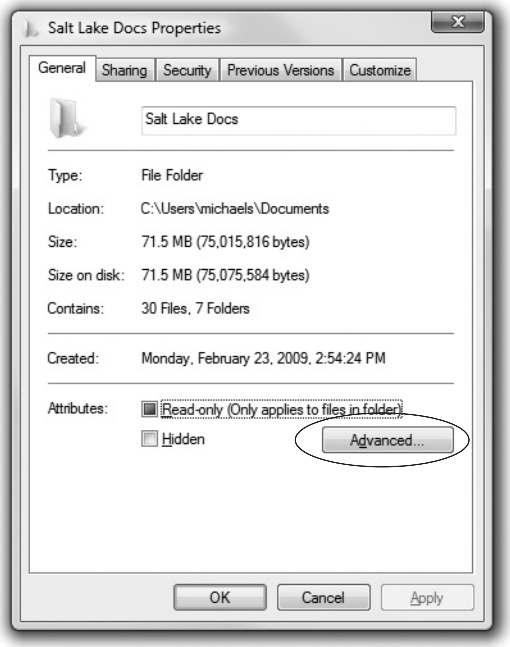
Protecting Data with Encryption

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 versions have basically no security features; Windows XP Professional uses the Encrypting File System to, well, encrypt files; and Windows Vista Ultimate and Enterprise add an encryption system that can encrypt entire hard drives.

Encrypting File System

The professional versions of Windows 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 versions 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 for that object, General tab, click the Advanced button (Figure 16-38) to open the Advanced Attributes dialog box. Click the check box next to *Encrypt contents to secure data* (Figure 16-39). 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.



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)

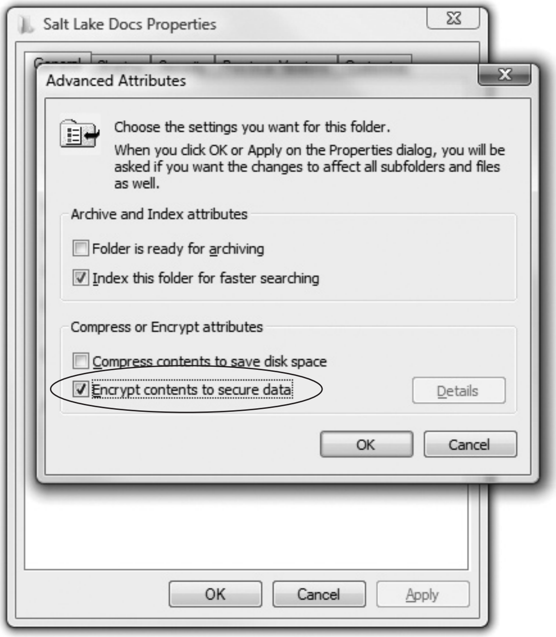
Contains: 30 Files, 7 Folders

Created: Monday, February 23, 2009, 2:54:24 PM

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

Figure 16-38 Click the Advanced button on the Properties, General tab

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



Salt Lake Docs Properties

Advanced Attributes

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

☑ Index this folder for faster searching

Compress or Encrypt attributes

□ Compress contents to save disk space

☑ Encrypt contents to secure data

Figure 16-39 Selecting encryption

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. You're out of luck.

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.

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 Ultimate and Enterprise editions offer full drive encryption through *BitLocker Drive Encryption*. BitLocker does 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 computer hasn't 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* (Figure 16-40).

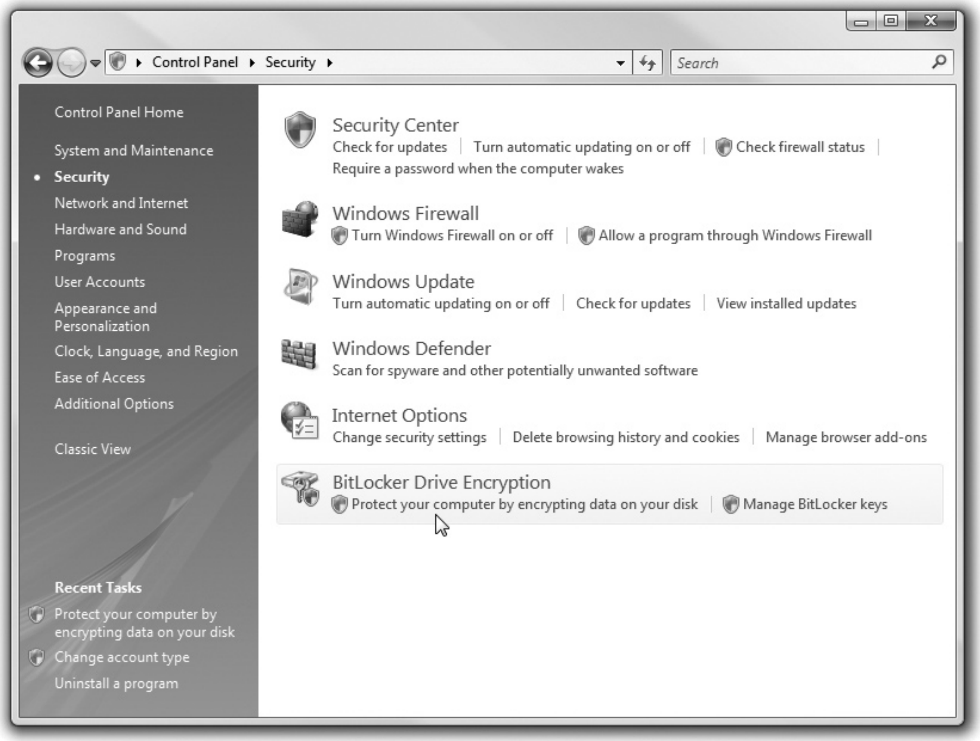

Control Panel ▸ Security ▸
Search
Control Panel Home
System and Maintenance
Security
Network and Internet
Hardware and Sound
Programs
User Accounts
Appearance and Personalization
Clock, Language, and Region
Ease of Access
Additional Options
Classic View
Recent Tasks
Protect your computer by encrypting data on your disk
Change account type
Uninstall a program
Security Center
Check for updates | Turn automatic updating on or off | Check firewall status | Require a password when the computer wakes
Windows Firewall
Turn Windows Firewall on or off | Allow a program through Windows Firewall
Windows Update
Turn automatic updating on or off | Check for updates | View installed updates
Windows Defender
Scan for spyware and other potentially unwanted software
Internet Options
Change security settings | Delete browsing history and cookies | Manage browser add-ons
BitLocker Drive Encryption
Protect your computer by encrypting data on your disk | Manage BitLocker keys

Figure 16-40 Enabling BitLocker Drive Encryption

Beyond A+

Aside from the tools available in Windows, you can find some excellent encryption tools readily downloadable. Arguably the best, most powerful of these tools is TrueCrypt.

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, you can 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 multi-boot 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 Home Premium, you can't get a better tool for securing your data.

Chapter Review Questions

1. Which of the following tools would enable you to create a new user account in Windows XP?

   A. User Accounts

   B. User Account Control

   C. Users and Groups

   D. Users and Passwords

2. Which feature in Windows XP enables you to change to another user account without logging out of the current user account?

   A. Change Accounts

   B. Fast User Switching

   C. User Account Control

   D. Users and Groups

3. Which is the best password for the user Joy, who has a pet named Fido and a birth date of January 8, 1982?

   A. joy1982

   B. joylovesfido

   C. 1982cutie

   D. oddvr88*

4. Members of the Users group in Windows 2000 can do which of the following?

   A. Create a group

   B. Manage all groups

   C. Edit the Registry

   D. Access critical system files

5. What feature in Windows Vista provides a permission dialog for Standard Users to enter administrator credentials to accomplish various tasks reserved for the latter group?

   A. User Access Command

   B. User Access Control

   C. User Account Command

   D. User Account Control

6. Which permission enables an administrator to change the ownership of a file without knowing the user account password for that file?

   A. Change permission

   B. Change Ownership permission

   C. Ownership permission

   D. Take Ownership permission

7. You copy a file from a folder on a hard drive formatted as NTFS, with permissions set to Read-only for everyone, to a USB thumb drive formatted as FAT32. What effective permissions does the copy of the file have?

   A. Read-only for everyone

   B. Full-control for everyone

   C. None

   D. You can't copy a file from an NTFS drive to a FAT32 drive.

8. What set of folders is available to all users on a computer in Windows XP?

   A. My Documents

   B. Personal Documents

   C. Public Folder

   D. Shared Documents

9. Which of the following operating systems do not allow you to disable Simple File Sharing? (Select two)
   - **A.** Windows XP Home
   - **B.** Windows XP Media Center
   - **C.** Windows XP Professional
   - **D.** Windows Vista Ultimate
10. Which of the following file systems enable you to encrypt an image, thus making it unviewable by any account but your own?
   - **A.** EFS
   - **B.** FAT
   - **C.** FAT32
   - **D.** OSR

Answers

1. **A.** User Accounts would enable you to create a new user account in Windows XP.
2. **B.** In Windows XP, Fast User Switching enables you to change to another user account without logging out of the current user account.
3. **D.** Of the choices listed, oddvr88* would be the best password; it has a non-alphanumeric character, which makes it more difficult for a hacker to crack.
4. **A.** Members of the Users group in Windows 2000 can create a group, but they can only manage groups that they create; they are not able to edit the Registry or access critical system files.
5. **D.** The User Account Control feature in Windows Vista provides a permission dialog for Standard Users to enter administrator credentials to accomplish various tasks normally reserved for the Administrators group.
6. **D.** The Take Ownership permission enables an administrator to change the ownership of a file without knowing the user account password for that file.
7. **C.** The key here is that you are copying from an NTFS hard drive to a FAT32 USB drive. Copying from an NTFS-based partition to a FAT- or FAT32-based partition creates two copies of the object; the copy of the object in the new location has no effective permissions at all.
8. **D.** The Shared Documents set of folders is available to all users on a computer in Windows XP.
9. **A, B.** Windows XP Home and Windows XP Media Center do not allow you to disable Simple File Sharing.
10. **A.** EFS file systems enable you to encrypt an image, thus making it unviewable by any account but your own.