CHAPTER 6

Getting the Most Out of User Accounts

Do you share your computer with other people either at work or at home? Then you're no doubt all too aware of one undeniable fact of human psychology: People are individuals with minds of their own! One person prefers Windows in a black-and-purple color scheme; another person just loves that annoying Peace wallpaper; yet another person prefers to have a zillion shortcuts on the Windows desktop; and, of course, everybody uses a different mix of applications. How can you possibly satisfy all those diverse tastes and prevent people from coming to blows?

It's a lot easier than you might think. Windows Vista lets you set up a different user account for each person who uses the computer. A **user account** is a username (and an optional password) that uniquely identifies a person who uses the system. The user account enables Windows Vista to control the user's **privileges**; that is, the user's access to system resources (**permissions**) and the user's ability to run system tasks (**rights**). Standalone and workgroup machines use *local* user accounts that are maintained on the computer, whereas domain machines use *global* user accounts that are maintained on the domain controller. This chapter looks at local user accounts.

Understanding Security Groups

Security for Windows Vista user accounts is handled mostly (and most easily) by assigning each user to a particular security group. For example, the built-in Administrator account and the user account you created during the Windows Vista setup process are part of the Administrators group. Each security group is defined with a specific set of

permissions and rights, and any user added to a group is automatically granted that group's permissions and rights. There are two main security groups:

> Administrators—Members of this group have complete control over the computer, meaning they can access all folders and files, install and uninstall programs (including legacy programs) and devices, create, modify, and remove user accounts, install Windows updates, service packs, and fixes, use Safe mode, repair Windows, take ownership of objects, and more.

> Users—Members of this group (also known as **Standard Users**) can access files only in their own folders and in the computer's shared folders, change their account's password, picture, and run programs and install programs that don't require administrative-level rights.

In addition to those groups, Windows Vista also defines up to 11 others that you'll use less often. Note that the permissions assigned to these groups are automatically assigned to members of the Administrators group. This means that if you have an administrator account, you don't also have to be a member of any other group in order to perform the task's specific to that group. Here's the list of groups:

> Backup Operators—Members of this group can access the Backup program and use it to back up and restore folders and files, no matter what permissions are set on those objects.

> Cryptographic Operators—Members of this group can perform cryptographic tasks.

> Distributed COM Users—Members of this group can start, activate, and use Distributed COM (DCOM) objects.

> Guests—Members of this group have the same privileges as those of the Users group. The exception is the default Guest account, which is not allowed to change its account password.

> IIS_USRS—Members of this group can work with a remote Internet Information Server.

> Network Configuration Operators—Members of this group have a subset of the Administrator-level rights that enables them to install and configure networking features.

> Performance Log Users—Members of this group can use the Windows Performance Diagnostic Console snap-in to monitor performance counters, logs, and alerts, both locally and remotely.

> Performance Monitor Users—Members of this group can use the Windows Performance Diagnostic Console snap-in to monitor performance counters only, both locally and remotely.

> Power Users—Members of this group (also known as **Standard Users**) have a subset of the Administrator group privileges. Power Users can't back up or restore files, replace system files, take ownership of files, or install or remove device drivers. In addition, Power

Users can't install applications that explicitly require the user to be a member of the Administrators group.

Remote Desktop Users—Members of this group can log on to the computer from a remote location using the Remote Desktop feature.

Replicator—Members of this group can replicate files across a domain.

Each user is also assigned a **user profile** that contains all the user's folders and files, as well as the user's Windows settings. The folders and files are stored in `\%SystemDrive%\Users\`*user*, where *user* is the username; for the current user, this folder is designated by the `%UserProfile%` variable. This location contains a number of subfolders that hold the user's document folders (Documents, Pictures, Music, and so on), desktop icons and subfolders (Desktop), Internet Explorer favorites (Favorites), contacts (Contacts), saved searches (Searches), and more.

There are also a number of user folders within the hidden `%UserProfile%\AppData` folder that contain the user's application data. Some are in `%UserProfile%\AppData\Local`, whereas others are in `%UserProfile%\AppData\Roaming` (supposedly because they'll be used with a **roaming profile**—a network-based user profile that enables you to log on to any computer and see your profile data. Table 6.1 lists some of the more important of these application data subfolders.

TABLE 6.1   Some Hidden User Profile Folders

Content	Location
Internet Explorer Cache	`\Local\Microsoft\Windows\Temporary Internet Files`
Internet Explorer History	`\Local\Microsoft\Windows\History`
Internet Explorer Cookies	`\Roaming\Microsoft\Windows\Cookies`
All Programs	`\Roaming\Microsoft\Windows\Start Menu\Programs`
Recent Items	`\Roaming\Microsoft\Windows\Recent`
Send To	`\Roaming\Microsoft\Windows\SendTo`
Start Menu	`\Roaming\Microsoft\Windows\Start Menu`
Startup	`\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`

User Account Control: Smarter User Privileges

New Most (I'm actually tempted to say the vast majority) of the security-related problems in recent versions of Windows boiled down to a single root cause: Most users were running Windows with administrator-level permissions. Administrators can do *anything* to a Windows machine, including installing programs, adding devices, updating drivers, installing updates and patches, changing Registry settings, running administrative tools, and creating and modifying user accounts. This is convenient, but it leads to a huge

problem: Any malware that insinuates itself onto your system will also be capable of operating with administrative permissions, thus enabling the program to wreak havoc on the computer and just about anything connected to it.

Windows XP tried to solve the problem by creating a second-tier account level called the **limited user**, which had only very basic permissions. Unfortunately, there were three gaping holes in this "solution":

▶ XP prompted you to create one or more user accounts during setup, but it didn't force you to create one. If you skipped this part, XP started under the Administrator account.

▶ Even if you elected to create users, the setup program didn't give you an option for setting the account security level. Therefore, any account you created during XP's setup was automatically added to the Administrators group.

▶ If you created a limited user account, you probably didn't keep it for long because XP hobbled the account so badly that you couldn't use it to do anything but the most basic computer tasks. You couldn't even install most programs because they generally require write permission for the `%SystemRoot%` folder and the Registry, and limited users lacked that permission.

Windows Vista tries once again to solve this problem. The new solution is called User Account Control and it uses a principle called the **least-privileged user**. The idea behind this is to create an account level that has no more permissions than it requires. Again, such accounts are prevented from editing the Registry and performing other administrative tasks. However, these users can perform other day-to-day tasks:

▶ Install programs and updates

▶ Add printer drivers

▶ Change wireless security options (such as adding a WEP or WPA key)

In Windows Vista, the least-privileged user concept arrives in the form of a new account type called the standard user. This means that Vista has three basic account levels:

▶ **Administrator account**—This built-in account can do anything to the computer.

▶ **Administrators group**—Members of this group (except the Administrator account) run as standard users but are able to elevate their privileges when required just by clicking a button in a dialog box (see the next section).

▶ **Standard users group**—These are the least-privileged users, although they, too, can elevate their privileges when needed. However, they require access to an administrator password to do so.

Elevating Privileges

This idea of elevating privileges is at the heart of Vista's new security model. In Windows Vista, you could use the Run As command to run a task as a different user (that is, one with higher privileges). In Vista, you usually don't need to do this because Vista prompts you for the elevation automatically.

If you're a member of the Administrators group, you run with the privileges of a standard user for extra security. When you attempt a task that requires administrative privileges, Vista prompts for your consent by displaying a User Account Control dialog box similar to the one shown in Figure 6.1. Click Control to permit the task to proceed. If this dialog box appears unexpectedly, it's possible that a malware program is trying to perform some task that requires administrative privileges; you can thwart that task by clicking Cancel instead.
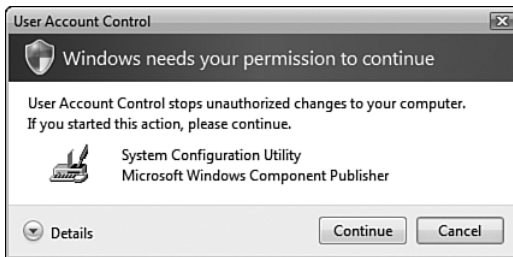

FIGURE 6.1   When an administrator launches a task that requires administrative privileges, Windows Vista displays this dialog box to ask for consent.

If you're running as a standard user and attempt a task that requires administrative privileges, Vista uses an extra level of protection. That is, instead of just prompting you for consent, it prompts you for the credentials of an administrator, as shown in Figure 6.2. If your system has multiple administrator accounts, each one is shown in this dialog box. Type the password for any administrator account shown, and then click Submit. Again, if this dialog box shows up unexpectedly, it might be malware, so you should click Cancel to prevent the task from going through.

Note, too, that in both cases Windows Vista switches to Secure Desktop mode, which means that you can't do anything else with Vista until you give your consent or credentials or cancel the operation. Vista indicates the secure desktop by darkening everything on the screen except the User Account Control dialog box.

> **NOTE**
>
> User Account Control seems eminently sensible on the surface, but Microsoft has not always implemented it in a sensible way. For example, sometimes you are prompted for elevation during simple tasks such as file deletions and renames, or when you change the system date or time. This has led to a backlash against User Account Control in some circles, and I'm sympathetic to a point. However, all the people who are complaining about User Account Control are Alpha Geeks who, by definition, are tweaking settings, installing drivers and programs, and generally pushing Vista to its

limits. Of course, you're going to get hit with lots of UAC dialog boxes under those conditions. However, the average user—even the average power user—doesn't tweak the system all that often, so I think UAC will be much less of a problem than its critics suggest.

FIGURE 6.2   When a standard user launches a task that requires administrative privileges, Windows Vista displays this dialog box to ask for administrative credentials.

As you saw in the "Running a Program with the Administrator Account" section of Chapter 5, "Installing and Running Applications," it's also possible to elevate your privileges for any individual program. You do this by right-clicking the program file or shortcut and then clicking Run as Administrator.

File and Registry Virtualization

You might be wondering how secure Windows Vista really is if a standard user can install programs. Doesn't that mean that malware can install as well? No—Vista implements a new model for installation security. In Vista, you need administrative privileges to write anything to the `%SystemRoot%` folder (usually `C:\Windows`), the `%ProgramFiles%` folder (usually `C:\Program Files`), and the Registry. Vista handles this for standard users in two ways:

▶ During a program installation, Vista first prompts the user for credentials (that is, Vista displays one of the Windows Security dialog boxes shown earlier in Figures 6.1 and 6.2). If they are provided, Vista gives permission to the program installer to write to `%SystemRoot%`, `%ProgramFiles%`, and the Registry.

▶ If the user cannot provide credentials, Vista uses a technique called **file and Registry virtualization**, which creates virtual `%SystemRoot%` and `%ProgramFiles%` folders, and a virtual `HKEY_LOCAL_MACHINE` Registry key, all of which are stored with the user's files. This enables the installer to proceed without jeopardizing actual system files.

User Account Control Policies

You can customize User Account Control to a certain extent by using group policies. In the Local Security Settings snap-in (press Windows Logo+R, type `secpol.msc`, click OK, and then provide your credentials), open the Security Settings, Local Policies, Security Options branch. Here you'll find nine policies related to User Account Control (as shown in Figure 6.3):

▸ **User Account Control: Admin Approval Mode for the Built-In Administrator Account**—This policy controls whether the Administrator account falls under User Account Control. If you enable this policy, the Administrator account is treated like any other account in the Administrators group and you must click Continue in the consent dialog box when Windows Vista requires approval for an action.

▸ **User Account Control: Behavior of the Elevation Prompt for Administrators in Admin Approval Mode**—This policy controls the prompt that appears when an administrator requires elevated privileges. The default setting is Prompt for Consent, where the user clicks either Continue or Cancel. You can also choose Prompt for Credentials to force the user to type his or her password. If you choose No Prompt, administrators cannot elevate their privileges.

▸ **User Account Control: Behavior of the Elevation Prompt for Standard Users**—This policy controls the prompt that appears when a standard user requires elevated privileges. The default setting is Prompt for Credentials, to force the user to type an administrator password. You can also choose No Prompt to prevent standard users from elevating their privileges.

▸ **User Account Control: Detect Application Installs and Prompt for Elevation**—Use this policy to enable or disable automatic privilege elevation while installing programs.

▸ **User Account Control: Only Elevate Executables That Are Signed and Validated**—Use this policy to enable or disable whether Vista checks the security signature of any program that asks for elevated privileges.

▸ **User Account Control: Only Elevate UIAccess Applications That Are Installed in Secure Locations**—Use this policy to enable or disable whether Vista allows elevation for accessibility applications that require access to the user interface of another window only if they are installed in a secure location (such as the `%ProgramFiles%` folder).

▸ **User Account Control: Run All Administrators in Admin Approval Mode**—Use this policy to enable or disable running administrators (excluding the Administrator account) as standard users.

▸ **User Account Control: Switch to the Secure Desktop When Prompting for Elevation**—Use this policy to enable or disable whether Vista switches to the secure desktop when the elevation prompts appear.

▶ **User Account Control: Virtualize File and Registry Write Failures to Per-User Locations**—Use this policy to enable or disable file and Registry virtualization for standard users.
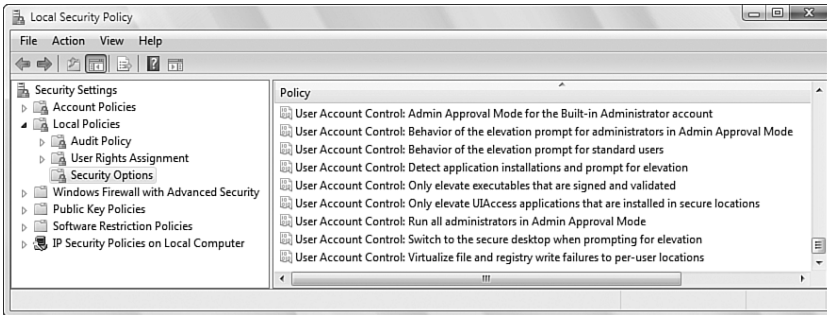

FIGURE 6.3   Vista policies related to User Account Control.

The rest of this chapter shows you the various methods Windows Vista offers to create, modify, and remove local user accounts.

Creating and Managing User Accounts

Windows Vista has a number of methods for working with user accounts. The most direct route is to use Control Panel's Manage Accounts window (select Start, Control Panel, Add or Remove User Accounts, and then enter your credentials). You create a new user account by following these steps:

1. Click Create a New Account. The Create New Account window appears.

2. Type the name for the account. The name can be up to 20 characters and must be unique on the system.

3. Activate either Administrator (to add the user to the Administrators group) or Standard User (to add the user to the Users group).

4. Click Create Account.

To modify an existing account, you have two choices:

▶ To modify your own account, click Go to the Main User Accounts Page to open the User Accounts window. Note that the links you see are slightly different from the ones listed next. For example, instead of Change Name, you see Change Your Name.

▶ To modify another user's account, click the account in the Manager Accounts window.

The latter technique opens the Change an Account window, shown in Figure 6.4, which includes some of or all the following tasks:

▶ **Change the Account Name**—Click this link to change the account's username. In the Rename Account window, type the new name and click Change Name.

▶ **Create a Password**—You see this task only if the user doesn't yet have an account password. Click the link to open the Create Password window, type the password twice, type a password hint, and then click Change Password.

> **NOTE**
>
> A strong password is the first line of defense when it comes to local computer security. Before setting up a password for an account, check out the section "Creating and Enforcing Bulletproof Passwords," later in this chapter.

> **CAUTION**
>
> The **password hint** is text that Vista displays in the Welcome screen if you type an incorrect password (see "Recovering from a Forgotten Password," later in this chapter). Because the hint is visible to anyone trying to log on to your machine, make the hint as vague as possible but still useful to you if you forget your password.

▶ **Change the Password**—If the user already has a password, click this link to change it. In the Change Password window, type the password twice, type a password hint, and then click Change Password.

▶ **Remove the Password**—If the user already has a password, click this link to delete it. In the Remove Password window, click Remove Password.

▶ **Change the Picture**—Click this link to change the random picture that Vista assigns to each account. In the Choose Picture window, either click one of the displayed images and then click Change Picture, or click Browse for More Pictures to use the Open dialog box to pick out an image from the Pictures folder (or wherever you like).

▶ **Set Up Parental Controls**—Click this link to apply Parental Controls to the user. See "Using Parental Controls to Restrict Computer Usage," later in this chapter.

▶ **Change the Account Type**—Click this link to open the Change Account Type window. Click either Standard User or Administrator and then click Change Account Type.

▶ **Delete the Account**—Click this link to delete the user account. In the Delete Account window, click either Delete Files or Keep Files (to delete or keep the user's documents), and then click Delete Account.

FIGURE 6.4   In the Manage Accounts window, click an account to see this list of tasks for changing the user's account.

Working with the User Accounts Dialog Box

Control Panel's User Accounts window has one major limitation: It offers only the Administrator and Limited (Users) account types. If you want to assign a user to one of the other groups, you have to use the User Accounts dialog box. You get there by following these steps:

1. Press Windows Logo+R (or select Start, All Programs, Accessories, Run) to display the Run dialog box.

2. In the Open text box, type `control userpasswords2`.

3. Click OK.

4. Enter your User Account Control credentials. Windows Vista displays the User Accounts dialog box, shown in Figure 6.5.

To enable the list of users, make sure that the Users Must Enter a User Name and Password to Use This Computer check box is activated.

Adding a New User

To add a new user via the User Accounts dialog box, follow these steps:

1. Click Add to launch the Add New User Wizard.

2. Type the new user's User Name (no more than 20 characters, and it must be unique). You can also type the user's Full Name and Description, but these are optional. Click Next.

3. Type the user's Password and type it again in the Confirm Password text box. Click Next.
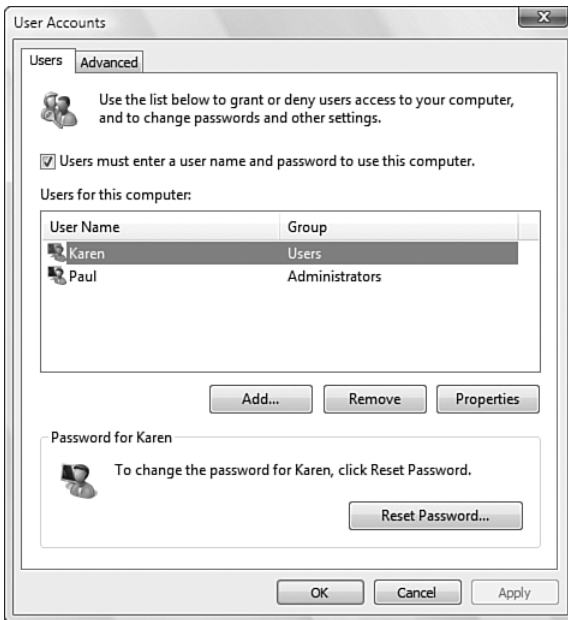
FIGURE 6.5   The User Accounts dialog box enables you to assign users to any Windows Vista security group.

   4. Activate the option that specifies the user's security group: Standard User (Users group), Administrator (Administrator group), or Other. Activate the latter to assign the user to any of the 13 default Windows Vista groups.

   5. Click Finish.

Performing Other User Tasks

Here's a list of the other tasks you can perform in the User Accounts dialog box:

   ▶ **Delete a user**—Select the user and click Remove. When Vista asks you to confirm, click Yes.

   ▶ **Change the user's name or group**—Select the user and click Properties to display the user's property sheet. Use the General tab to change the username; use the Group Membership tab to assign the user to a different group. Note that you can only assign the user to a single group using this method. If you need to assign a user to multiple groups, see "Working with the Local Users and Groups Snap-In," next.

   ▶ **Change the user's password**—Select the user and click Reset Password. Type the password in the New Password and Confirm New Password text boxes and click OK.

Working with the Local Users and Groups Snap-In

The most powerful of the Windows Vista tools for working with users is the Local Users and Groups MMC snap-in. To load this snap-in, Vista offers three methods:

▶ In the User Accounts dialog box (refer to the previous section), display the Advanced tab and then click the Advanced button.

▶ Press Windows Logo+R (or select Start, All Programs, Accessories, Run) type **lusrmgr.msc**, and click OK.

▶ Select Start, right-click Computer, and then click Manage. In the Computer Management window, select System Tools, Local Users and Groups.

Whichever method you use, enter your credentials and then select the Users branch to see a list of the users on your system, as shown in Figure 6.6.
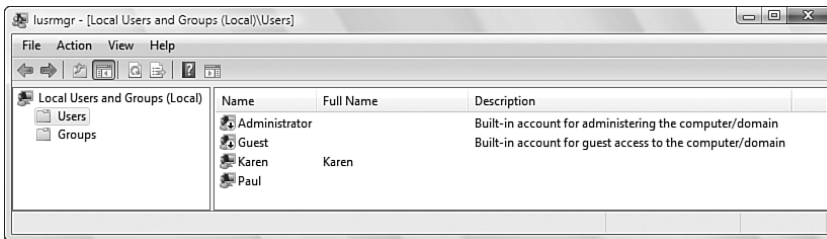

FIGURE 6.6   The Users branch lists all the system's users and enables you to add, modify, and delete users.

From here, you can perform the following tasks:

▶ **Add a new user**—Make sure that no user is selected and then select Action, New User. In the New User dialog box, type the User Name, Password, and Confirm Password. (I discuss the password-related check boxes in this dialog box later in this chapter; see "User Account Password Options.") Click Create.

▶ **Change a user's name**—Right-click the user and then click Rename.

▶ **Change a user's password**—Right-click the user and then click Set Password.

▶ **Add a user to a group**—Double-click the user to open the user's property sheet. In the Member Of tab, click Add and use the Enter the Object Names to Select box to enter the group name. If you're not sure of the name, click Advanced to open the Select Groups dialog box, click Find Now to list all the groups, select the group, and then click OK. Click OK to close the property sheet.

> **NOTE**
>
> Another way to add a user to a group is to select the Groups branch in the Local Users and Groups snap-in. Right-click the group you want to work with, and then click Add to Group. Now click Add, type the username in the Enter the Object Names to Select box, and then click OK.

- ▶ **Remove a user from a group**—Double-click the user to open the user's property sheet. In the Member Of tab, select the group from which you want the user removed, and then click Remove. Click OK to close the property sheet.

- ▶ **Change a user's profile**—Double-click the user to open the user's property sheet. Use the Profile tab to change the profile path, logon script, and home folder (activate the Local Path option to specify a local folder; or activate Connect to specify a shared network folder).

- ▶ **Disable an account**—Double-click the user to open the user's property sheet. In the General tab, activate the Account Is Disabled check box.

- ▶ **Delete a user**—Right-click the user and then click Delete. When Vista asks you to confirm, click Yes.

Setting Account Policies

Windows Vista Pro offers several sets of policies that affect user accounts. There are three kinds of account policies: security options, user rights, and account lockout policies. The next three sections take you through these policies.

Setting Account Security Policies

To see these policies, you have two choices:

- ▶ Open the Group Policy editor (press Windows Logo+R, type `gpedit.msc`, and click OK) and select Computer Configuration, Windows Settings, Security Settings, Local Policies, Security Options, as shown in Figure 6.7.

- ▶ Launch the Local Security Settings snap-in (press Windows Logo+R, type `secpol.msc`, and click OK) and select Security Settings, Local Policies, Security Options.

The Accounts grouping has five policies:

- ▶ **Administrator Account Status**—Use this policy to enable or disable the Administrator account. This is useful if you think someone else might be logging on as the Administrator. (A less drastic solution would be to change the Administrator password or rename the Administrator account.)
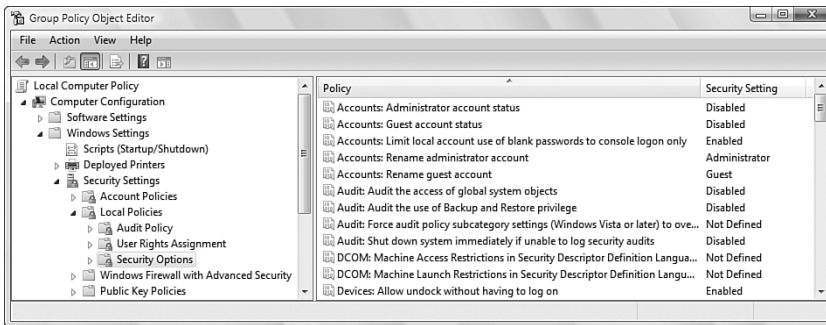
FIGURE 6.7   In the Security Options branch, use the five Accounts policies to configure security for your accounts.

> **NOTE**
>
> The Administrator account is always used during a Safe Mode boot, even if you disable the account.

▶ **Guest Account Status**—Use this option to enable or disable the Guest account.

▶ **Limit Local Account Use of Blank Passwords to Console Logon Only**—When this option is enabled, Windows Vista allows users with blank passwords to log on to the system directly only by using the Welcome screen. Such users can't log on via either the `RunAs` command or remotely over a network. This policy modifies the following Registry setting:

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\limitblankpassworduse
```

▶ **Rename Administrator Account**—Use this option to change the name of the Administrator account.

▶ **Rename Guest Account**—Use this option to change the name of the Guest account.

Setting User Rights Policies

Windows Vista has a long list of policies associated with user rights. To view these policies, you have two choices:

▶ In the Group Policy editor, select Computer Configuration, Windows Settings, Security Settings, Local Policies, User Rights Assignment, as shown in Figure 6.8.

▶ In the Local Security Policy snap-in, select Security Settings, Local Policies, User Rights Assignment.
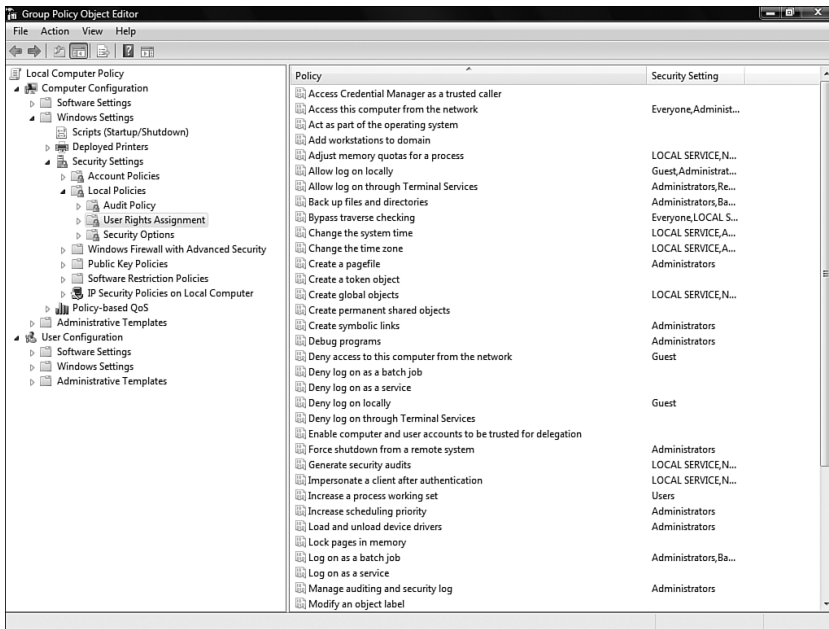
FIGURE 6.8   In the User Rights Assignment branch, use the policies to configure the rights assigned to users or groups.

Each policy is a specific task or action, such as Back Up Files and Directories, Deny Logon Locally, and Shut Down the System. For each task or action, the Security Setting column shows the users and groups who can perform the task or to whom the action applies. To change the setting, double-click the policy. Click Add User or Group to add an object to the policy; or delete an object from the policy by selecting it and clicking Remove.

Setting Account Lockout Policies

Last of all, Windows Vista has a few policies that determine when an account gets **locked out**, which means the user is unable to log on. A lock out occurs when the user fails to log on after a specified number of attempts. This is a good security feature because it prevents an unauthorized user from trying a number of different passwords. Use either of the following methods to view these policies:

▶ In the Group Policy editor, select Computer Configuration, Windows Settings, Security Settings, Account Policies, Account Lockout Policy, as shown in Figure 6.9.

▶ In the Local Security Policy snap-in, select Security Settings, Account Policies, Account Lockout Policy.
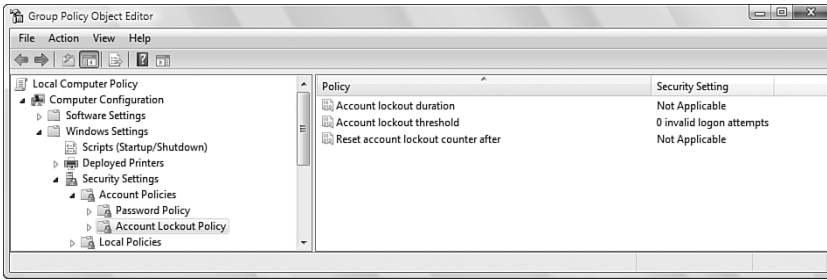
FIGURE 6.9   In the Account Lockout Policy branch, use the policies to configure when an account gets locked out of the system.

There are three policies:

▶ **Account Lockout Duration**—This policy sets the amount of time, in minutes, that the user is locked out. Note that, to change this policy, you must set the Account Lockout Threshold (described next) to a nonzero number.

▶ **Account Lockout Threshold**—This policy sets the maximum number of logons the user can attempt before being locked out. Note that after you change this to a nonzero value, Windows Vista offers to set the other two policies to 30 minutes.

▶ **Reset Account Lockout Counter After**—This policy sets the amount of time, in minutes, after which the counter that tracks the number of invalid logons is reset to 0.

Working with Users and Groups from the Command Line

You can script your user and group chores by taking advantage of the NET USER and NET LOCALGROUP commands. These commands enable you to add users, change passwords, modify accounts, add users to groups, and remove users from groups. Note that you must run these commands under the Administrator account, so first follow these steps to open a command prompt session:

1. Select Start, All Programs, Accessories.

2. Right-click Command Prompt and then click Run as Administrator.

3. Enter your User Account Control credentials.

The NET USER Command

You use the NET USER command to add users, set account passwords, disable accounts, set account options (such as the times of day the user is allowed to log on), and remove accounts. For local users, the NET USER command has the following syntax:

```
NET USER [username [password ¦ * ¦ /RANDOM] [/ADD] [/DELETE] [options]]
```

username   The name of the user you want to add or work with. If you run NET USER
               with only the name of an existing user, the command displays the user's
               account data.

password   The password you want to assign to the user. If you use *, Windows Vista
               prompts you for the password; if you use the /RANDOM switch, Windows
               Vista assigns a random password (containing eight characters, consisting
               of a random mix of letters, numbers, and symbols), and then displays the
               password on the console.

/ADD   Creates a new user account.

/DELETE   Deletes the specified user account.

options   These are optional switches you can append to the command:

               /ACTIVE:{YES ¦ NO}   Specifies whether the account is active or
                                           disabled.

               /EXPIRES:{*date* ¦ NEVER}   The date (expressed in the system's Short
                                           Date format) on which the account expires.

               /HOMEDIR:*path*   The home folder for the user, which should
                                           be a subfolder within %SystemDrive%\Users
                                           (make sure that the folder exists).

               /PASSWORDCHG:{YES ¦ NO}   Specifies whether the user is allowed to
                                           change his password.

               /PASSWORDREQ:{YES ¦ NO}   Specifies whether the user is required to
                                           have a password.

               /PROFILEPATH:*path*   The folder that contains the user's profile.

               /SCRIPTPATH:*path*   The folder that contains the user's logon
                                           script.

               /TIMES:{*times* ¦ ALL}   Specifies the times that the user is allowed
                                           to log on to the system. Use single days or
                                           day ranges (for example, Sa or M-F). For
                                           times, use 24-hour notation or 12-hour nota-
                                           tion with am or pm. Separate the day and
                                           time with a comma, and separate day/time
                                           combinations with semicolons. Here are
                                           some examples:

                                               M-F,9am-5pm
                                               M,W,F,08:00-13:00
                                               Sa,12pm-6pm;Su,1pm-5pm

> **CAUTION**
>
> If you use the /RANDOM switch to create a random password, be sure to make a note of the new password so that you can communicate it to the new user.

Note, too, that if you execute NET USER without any parameters, it displays a list of the local user accounts.

> **TIP**
>
> If you want to force a user to log off when his logon hours expire, open the Group Policy editor and select Computer Configuration, Windows Settings, Security Settings, Local Policies, Security Options. In the Network Security category, enable the Force Logoff When Logon Hours Expire policy.

The NET LOCALGROUP Command

You use the NET LOCALGROUP command to add users to and remove users from a specified security group. NET LOCALGROUP has the following syntax:

```
NET LOCALGROUP [group name1 [name2 ...] {/ADD ¦ /DELETE}
```

group	This is the name of the security group with which you want to work.
name1 [*name2* ...]	One or more usernames that you want to add or delete, separated by spaces.
/ADD	Adds the user or users to the group.
/DELETE	Removes the user or users from the group.

Creating and Enforcing Bulletproof Passwords

Windows Vista sometimes gives the impression that passwords aren't all that important. After all, the user account you specify during setup is supplied with administrative-level privileges *and* a password is optional. That's a dangerous setup, because it means that anyone can start your computer and automatically get administrative rights, and that standard users can elevate permissions without needing a password. However, these problems are easily remedied by supplying a password to *all* local users. This section gives you some pointers for creating strong passwords and runs through Windows Vista's password-related options and policies.

Creating a Strong Password

Ideally, when you're creating a password for a user, you want to pick one that that provides maximum protection without sacrificing convenience. Keeping in mind that the

whole point of a password is to select one that nobody can guess, here are some guidelines you can follow when choosing a password:

> **TIP**
>
> Consider submitting a password similar to (but *not* the same as) the one you want to use to an online password complexity checker. I use Microsoft's (www.microsoft.com/athome/security/privacy/password_checker.mspx), but a Google search on "password complexity checker" will reveal any others.

- ▶ **Use passwords that are at least eight characters long**—Shorter passwords are susceptible to programs that just try every letter combination. You can combine the 26 letters of the alphabet into about 12 million different five-letter word combinations, which is no big deal for a fast program. If you bump things up to eight-letter passwords, however, the total number of combinations rises to 200 *billion*, which would take even the fastest computer quite a while. If you use 12-letter passwords, as many experts recommend, the number of combinations goes beyond mind-boggling: 90 *quadrillion*, or 90,000 trillion!

- ▶ **Don't be too obvious**—Because forgetting a password is inconvenient, many people use meaningful words or numbers so that their password will be easier to remember. Unfortunately, this means that they often use extremely obvious things such as their name, the name of a family member or colleague, their birth date or Social Security number, or even their system username. Being this obvious is just asking for trouble.

- ▶ **Don't use single words**—Many crackers break into accounts by using "dictionary programs" that just try every word in the dictionary. So, yes, *xiphoid* is an obscure word that no person would ever guess, but a good dictionary program will figure it out in seconds flat. Using two or more words in your password (or **pass phrase**, as multiword passwords are called) is still easy to remember, and would take much longer to crack by a brute force program.

- ▶ **Use a misspelled word**—Misspelling a word is an easy way to fool a dictionary program. (Make sure, of course, that the resulting arrangement of letters doesn't spell some other word.)

- ▶ **Mix uppercase and lowercase letters**—Windows Vista passwords are case-sensitive, which means that if your password is, say, *YUMMY ZIMA*, trying *yummy zima* won't work. You can really throw snoops for a loop by mixing the case. Something like *yuMmY zIMa* would be almost impossible to figure out.

- ▶ **Add numbers to your password**—You can throw more permutations and combinations into the mix by adding a few numbers to your password.

- ▶ **Include a few punctuation marks and symbols**—For extra variety, toss in one or more punctuation marks or special symbols, such as % or #.

▶ **Try using acronyms**—One of the best ways to get a password that appears random but is easy to remember is to create an acronym out of a favorite quotation, saying, or book title. For example, if you've just read *The Seven Habits of Highly Effective People*, you could use the password T7HoHEP.

▶ **Don't write down your password**—After going to all this trouble to create an inde-structible password, don't blow it by writing it on a sticky note and then attaching it to your keyboard or monitor! Even writing it on a piece of paper and then throw-ing the paper away is dangerous. Determined crackers have been known to go through a company's trash looking for passwords (this is known in the trade as **Dumpster diving**). Also, don't use the password itself as your Windows Vista pass-word hint.

▶ **Don't tell your password to anyone**—If you've thought of a particularly clever password, don't suddenly become unclever and tell someone. Your password should be stored in your head alongside all those "wasted youth" things you don't want anyone to know about.

▶ **Change your password regularly**—If you change your password often (say, once a month or so), even if some skulker does get access to your account, at least he'll have it for only a relatively short period.

User Account Password Options

Each user account has a number of options related to passwords. To view these options, open the Local Users and Groups snap-in (as described earlier in this chapter), and double-click the user with which you want to work. There are three password-related check boxes in the property sheet that appears:

User Must Change Password at Next Logon—If you activate this check box, the next time the user logs on, she will see a dialog box with the message that she is required to change her password. When the user clicks OK, the Change Password dialog box appears and the user enters her new password.

User Cannot Change Password—Activate this check box to prevent the user from chang-ing the password.

Password Never Expires—If you deactivate this check box, the user's password will expire. The expiration date is determined by the Maximum Password Age policy, discussed in the next section.

Taking Advantage of Windows Vista's Password Policies

Windows Vista maintains a small set of useful password-related policies that govern settings such as when passwords expire and the minimum length of a password. There are two methods you can use to view these policies:

▶ In the Group Policy editor, select Computer Configuration, Windows Settings, Security Settings, Account Policies, Password Policy, as shown in Figure 6.10.

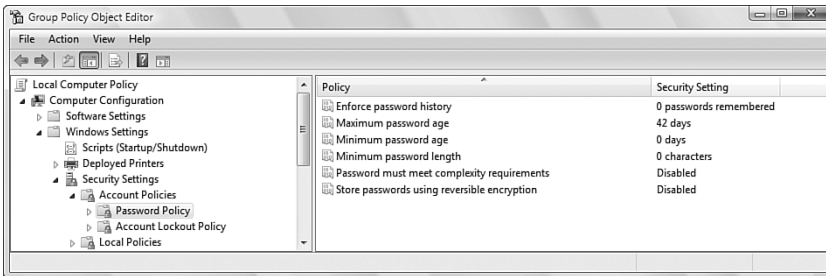▶ In the Local Security Policy snap-in, select Security Settings, Account Policies, Password Policy.

FIGURE 6.10   In the Password Policy branch, use the policies to enforce strong passwords and other protections.

There are six policies:

▶ **Enforce Password History**—This policy determines the number of old passwords that Windows Vista stores for each user. This is to prevent a user from reusing an old password. For example, if you set this value to 10, the user can't reuse a password until he or she has used at least 10 other passwords. Enter a number between 0 and 24.

▶ **Maximum Password Age**—This policy sets the number of days after which passwords expire. This applies only to user accounts where the Password Never Expires property has been disabled (refer to the previous section). Enter a number between 1 and 999.

▶ **Minimum Password Age**—This policy sets the numbers of days that a password must be in effect before the user can change it. Enter a number between 1 and 998 (but less than the Maximum Password Age value).

▶ **Minimum Password Length**—This policy sets the minimum number of characters for the password. Enter a number between 0 and 14 (where 0 means no password is required).

▶ **Password Must Meet Complexity Requirements**—If you enable this policy, Windows Vista examines each new password and accepts it only if it meets the following criteria: It doesn't contain all or part of the username; it's at least six characters long; and it contains characters from three of the following four categories: uppercase letters, lowercase letters, digits (0–9), and nonalphanumeric characters (such as $ and #).

▶ **Store Passwords Using Reversible Encryption**—Enabling this policy tells Windows Vista to store user passwords using reversible encryption. Some applications require this, but they're rare and you should never need to enable this policy because it makes your passwords much less secure.

CAUTION

Reversible encryption means that data is encrypted using a particular code as a seed value, and you can then decrypt the data by applying that same code. Unfortunately, this type of encryption has been cracked, and programs to break reversible encryption are easy to find on the Net. This means that hackers with access to your system can easily decrypt your password store and see all your passwords. Therefore, you should never enable the Store Passwords Using Reversible Encryption policy.

Recovering from a Forgotten Password

Few things in life are as frustrating as a forgotten password. To avoid this headache, Windows Vista offers a couple of precautions that you can take now just in case you forget your password.

The first precaution is called the password hint, discussed earlier (refer to "Creating and Managing User Accounts"), which is a word, phrase, or other mnemonic device that can help you remember your password. To see the hint in the Welcome screen, type any password and press Enter. When Vista tells you the password is incorrect, click OK. Vista redisplays the Password text box with the hint below it.

The second precaution you can take is the Password Reset Disk. This is a floppy disk that enables you to reset the password on your account without knowing the old password. To create a Password Reset Disk, follow these steps:

1. Log on as the user for whom you want to create the disk.

2. Select Start, Control Panel, User Accounts and Family Safety, User Accounts.

3. In the Tasks pane, click Create a Password Reset Disk. This launches the Forgotten Password Wizard.

4. Run through the wizard's dialog boxes. (Note that you'll need a blank, formatted floppy disk.)

The password reset disk contains a single file named `Userkey.psw`, which is an encrypted backup version of your password. Be sure to save this disk in a secure location and, just to be safe, don't label the disk. If you need to use this disk, follow these steps:

1. Start Windows Vista normally.

2. When you get to the Welcome screen, leave your password blank and press the Enter key. Windows Vista will then tell you the password is incorrect.

3. Click OK.

4. Click the Reset Password link.

5. In the initial Password Reset Wizard dialog box, click Next.

6. Insert the password reset disk and click Next.

7. Type a new password (twice), type a password hint, and click Next.

8. Click Finish.

Sharing Files with Other Users

Vista Home Basic   Each user has his or her own profile, which means (in part) his or her own user folders, and Vista requires administrator-level credentials for one user to mess with another user's folders. If you want to share files with other users, Vista gives you two methods: the Public folder and Sharing. The latter is the same as network sharing, so see Chapter 23's "Sharing Resources with the Network" section.

Unfortunately, Vista doesn't make it easy to get to the Public folder, for some reason. The only route is to open any folder window, click the top-level drop-down list in the address bar (as shown in Figure 6.11), and then click Public.
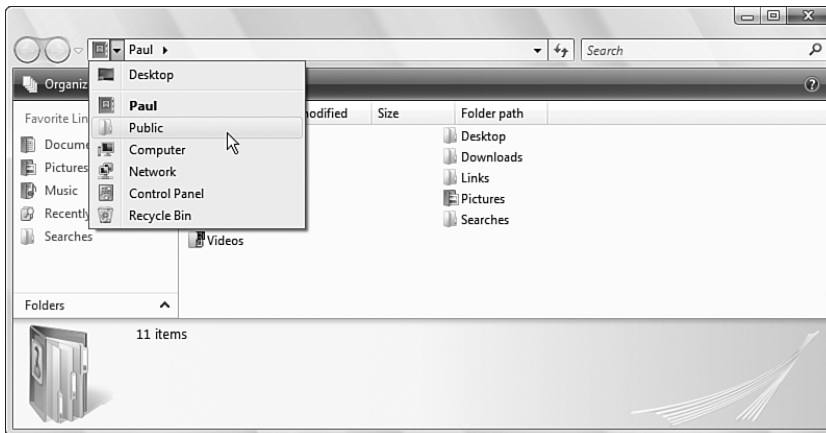

FIGURE 6.11   To get to the hard-to-find Public folder, in any folder window, drop-down the list for the address bar's top-level item and then click Public.

Figure 6.12 shows the Public folder and its subfolders. To share a file with other users, copy (or cut) it from its original folder and paste it in one of the Public subfolders.
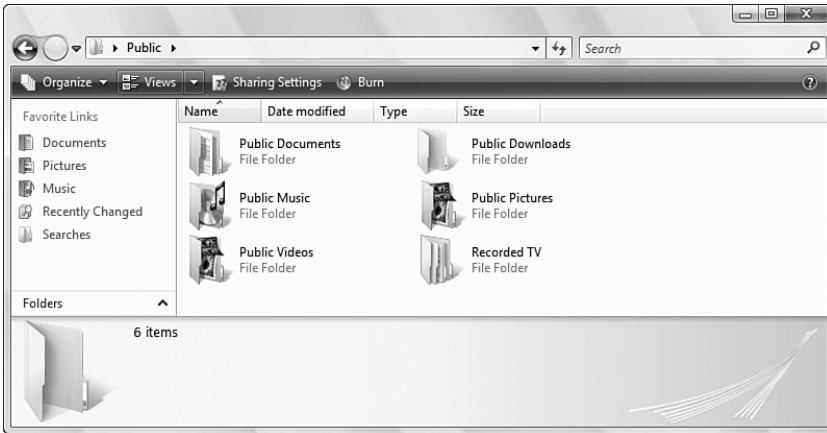
FIGURE 6.12   Copy or move a file to one of the Public subfolders to share the file with other users.

Using Parental Controls to Restrict Computer Usage

If you have children who share your computer, or if you're setting up a computer for the kids' use, it's wise to take precautions regarding the content and programs that they can access. Locally, this might take the form of blocking access to certain programs (such as your financial software), using ratings to control which games they can play, and setting time limits on when the computer is used. If the computer has Internet access, you might also want to allow (or block) specific sites, block certain types of content, and prevent file downloads.

Vista **Home Basic**   Vista **Home Premium**   Vista **Ultimate Edition**

All this sounds daunting, but Windows Vista's new Parental Controls make things a bit easier by offering an easy-to-use interface that lets you set all of the aforementioned options and lots more. (You get Parental Controls in the Home Basic, Home Premium, and Ultimate editions of Windows Vista.)

Before you begin, be sure to create a standard user account for each child that uses the computer. When that's done, you get to Parental Controls by select Start, Control Panel, Set Up Parental Controls. Enter your credentials to get to the Parental Controls window, and then click the user you want to work with to get to the User Controls window.

Activating Parental Controls and Activity Reporting

You should activate two options here (see Figure 6.13):

▶ **Parental Controls**—Click On, Enforce Current Settings. This enables the Windows Vista Web Filter, and the Time Limits, Games, and Allow and Block Specific Programs links in the Settings area.

▶ **Activity Reporting**—Click On, Collect Information About Computer Usage. This tells Vista to track system events such as blocked logon attempts and attempted changes to user accounts, system date and time, and system settings.
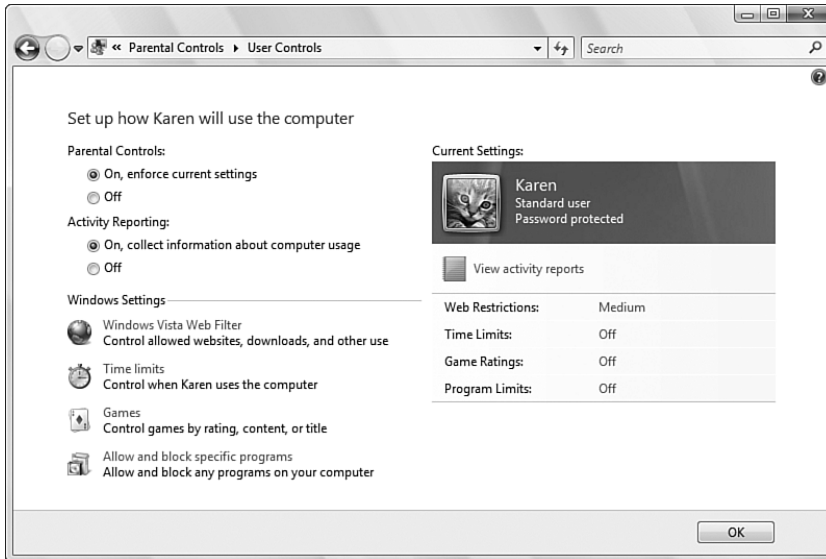

FIGURE 6.13   The User Controls page enables you to set up web, time, game, and program restrictions for the selected user.

The User Controls window gives you four links to use when setting up the controls for this user:

▶ **Windows Vista Web Filter**—Click this link to display the Web Restrictions page. Here you can allow or block specific websites, set up general site restrictions (High, Medium, None, or Custom), and block file downloads. If you select the Custom Web restriction level, then you can also block specific content categories (such as Pornography, Mature Content, and Bomb Making).

TIP

To make your life easier, you can import lists of allowed or blocked sites. First, create a new text file and change the extension to `Web Allow Block List` (for example, `MyURLs.Web Allow Block List`). Open the file and add the following text to start:

```
<WebAddresses>
</WebAddresses>
```

Between these lines, add a new line for each site using the following format:

```
<URL AllowBlock="n">address</URL>
```

Replace *n* with 1 for a site you want to allow, or 2 for a site you want to block, and replace *address* with the site URL. Here's an example:

```
<WebAddresses>
<URL AllowBlock="1">http://www.goodcleanfun.com</URL>
<URL AllowBlock="1">http://www.wholesomestuff.com</URL>
<URL AllowBlock="2">http://www.smut.com</URL>
<URL AllowBlock="2">http://www.depravity.com</URL>
</WebAddresses>
```

NOTE

If the user is logged on when a restricted time approaches, an icon appears in the notification area to let that user know. If the user is still logged on when the restricted time occurs, the user is immediately logged off and cannot log back on until the restricted time has passed. Fortunately, Vista is kind enough to restore the user's programs and documents when he or she logs back on.

▶ **Time Limits**—Click this link to display the Time Restrictions page, which shows a grid where each square represents an hour during the day for each day of the week, as shown in Figure 6.14. Click the squares to block computer usage during the selected times.

▶ **Games**—Click this link to display the Game Controls page. Here you can allow or disallow all games, restrict games based on ratings and contents, and block or allow specific games. You'll see how this works in the next section.

▶ **Allow and Block Specific Programs**—Click this link to display the Application Restrictions page, which displays a list of the programs on your computer. Activate the *User* Can Only Use the Programs I Allow option and then click the check boxes for the programs you want to allow the person to use.

Example: Setting Up Parental Controls for Games

If you have kids, chances are, they have a computer—either their own or one shared with the rest of the family—and, chances are, they play games on that computer. That's not a problem when they are being supervised, but few of us have the time or energy to sit beside our kids for each and every computer session—and the older the kid, the more likely that a hovering adult will be seen as an interloper. In other words, for all but the youngest users, your children will have some unsupervised gaming time at the computer.
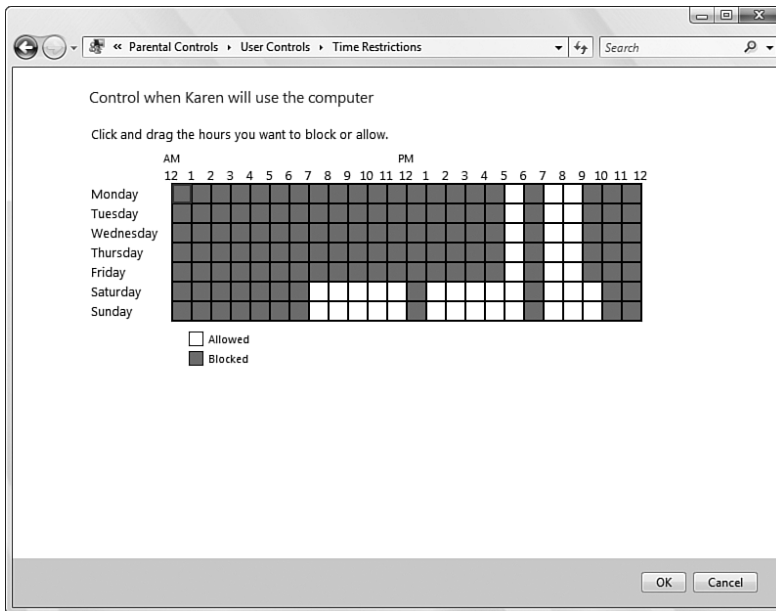
FIGURE 6.14   Use the grid on the Time Restrictions page to block computer access during specified hours.

To avoid worrying about whether your 8-year-old is playing Grand Theft Auto or something equally unsuitable, you can take advantage of the Game Controls section that enables you to control gaming using ratings and content descriptors.

Before setting up the controls, you should select the rating system you want to use. Return to the Parental Controls window and then click the Select a Games Ratings System link to display the Game Rating Systems window shown in Figure 6.15. Select the rating system you prefer and then click OK to return to the Parent Controls window.

Click the user you want to work with to display the User Controls window. Activate the On, Enforce Current Settings option (if you haven't done so already), and then click Games to display the Game Controls window, shown in Figure 6.16.

The next three sections run through the three methods you can use to control game play.

Turn Off Game Play

If your kids are too young to play any games, or if you'd prefer that they spend time on the computer working on more constructive pursuits, you can turn off game playing altogether. In the Can *UserName* Play Games? section, select No to prevent the user named *UserName* from launching any games from the Games Explorer. If you select Yes instead, you can use the techniques in the next two sections to control the games the user can play.
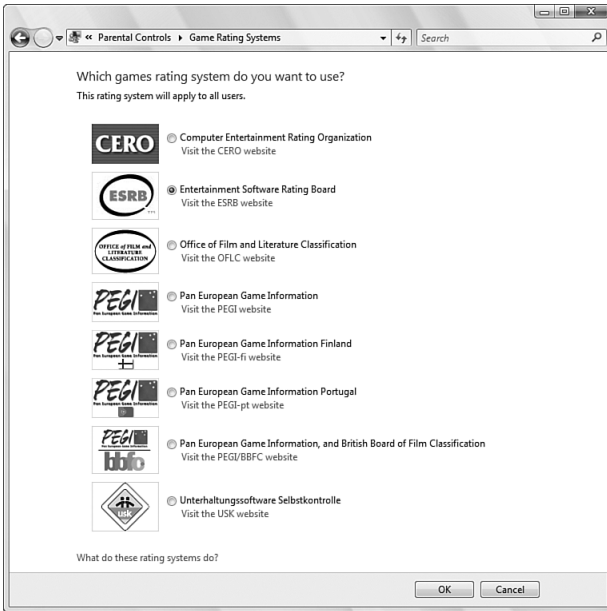
FIGURE 6.15   Use the Game Rating Systems window to choose the rating system you want to use with parental controls.
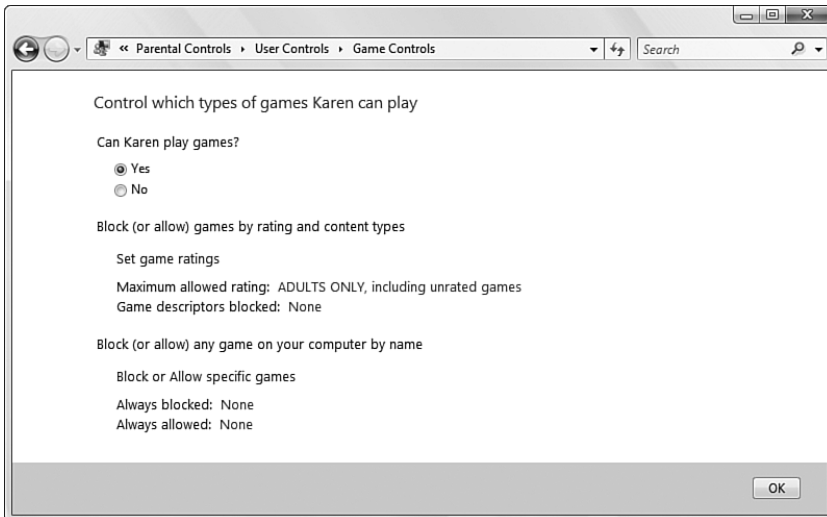

FIGURE 6.16   Use the Game Controls window to set the gaming restrictions for the selected user.

Controlling Games via Ratings and Descriptors

Instead of shutting off all game play, you're more likely to want to prevent each user from playing certain types of games. The easiest way to do that is to use game ratings and content descriptors. In the Game Controls window, click Set Game Ratings to display the Game Restrictions window, shown in Figure 6.17.
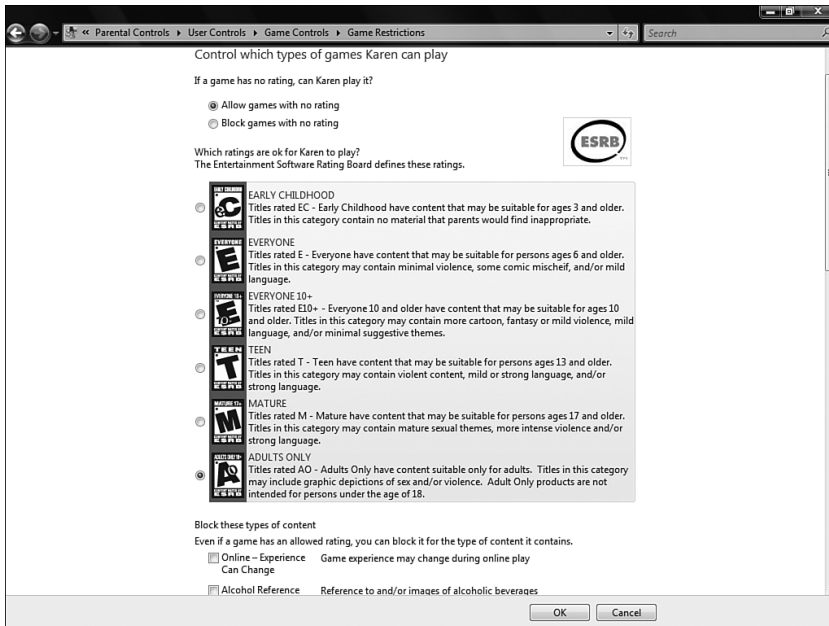

FIGURE 6.17   Use the Game Restrictions window to control game playing using ratings and content descriptors.

Click the rating option that represents the highest rating the user is allowed to play. For example, if you're using the ESRB rating system and you select the Teen option, the user will be able to play games rated as Early Childhood, Everyone, Everyone 10+, and Teen. He or she will not be able to play games rated as Mature or Adults Only.

You can also prevent the user from playing unrated games by selecting the Block Games with No Rating option.

You can also block games based on content descriptors. If you scroll down in the Game Restrictions window, you see the complete set of content descriptors, each with its own check box. For each check box you activate, the user will not be able to run any games that include that content description, even if the game has a rating that you allow.

Blocking and Allowing Specific Games

You might want to fine-tune your game controls by overriding the restrictions you've set up based on ratings and content descriptors. For example, you might have activated the Block Games with No Rating option, but you have an unrated game on your system that

you want to allow the kids to play. Similarly, there might be a game that Vista allows based on the ratings and descriptors, but you'd feel more comfortable blocking access to the game.

In the Game Controls window, click Block or Allow Specific Games to display the Game Overrides window, shown in Figure 6.18. The table displays the title and rating of your installed games, and shows the current control status—Can Play or Cannot Play. To allow the user to play a specific game, click Always Allow; to prevent the user from playing a specific game, click Always Block.
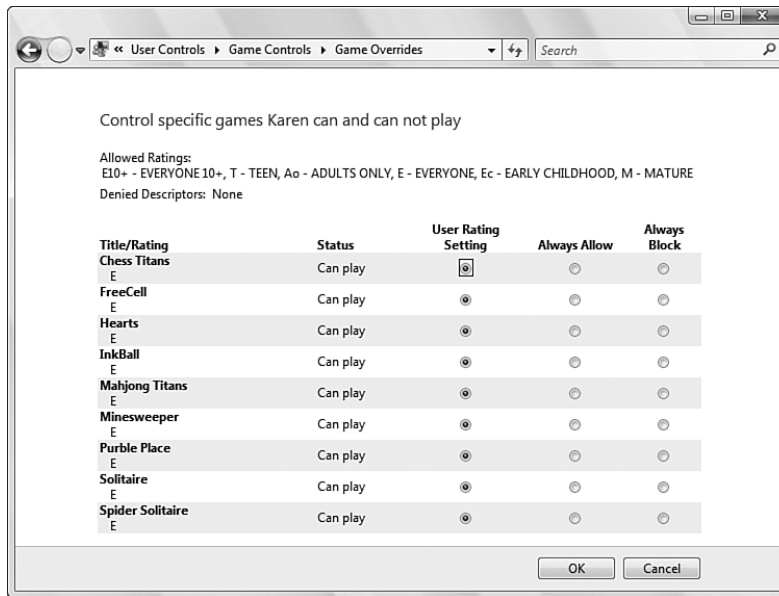

FIGURE 6.18   Use the Game Overrides window to allow or block specific games.

Sharing Your Computer Securely

If you're the only person who uses your computer, you don't have to worry all that much about the security of your user profile—that is, your files and Windows Vista settings. However, if you share your computer with other people, either at home or at the office, you need to set up some kind of security to ensure that each user has his "own" Windows and can't mess with anyone else's (either purposely or accidentally). Here's a list of security precautions to set up when sharing your computer (these techniques have been discussed earlier in this chapter, except where noted):

▶ **Create an account for each user**—Everyone who uses the computer, even if they use it only occasionally, should have her own user account. (If a user needs to access the computer rarely, or only once, activate the Guest account and let him use that. You should disable the Guest account after the user finishes his session.)

▶ **Remove unused accounts**—If you have accounts set up for users who no longer require access to the computer, you should delete those accounts.

▶ **Limit the number of administrators**—Members of the Administrators group can do *anything* in Windows Vista simply by clicking Submit in the User Account Control dialog box. These powerful accounts should be kept to a minimum. Ideally, your system should have just one (besides the built-in Administrator account).

▶ **Rename the Administrator account**—Renaming the Administrator account ensures that no other user can be certain of the name of the computer's top-level user.

▶ **Put all other accounts in the Users (Standard users) group**—Most users can perform almost all of their everyday chores with the permissions and rights assigned to the Users group, so that's the group you should use for all other accounts.

▶ **Use strong passwords on all accounts**—Supply each account with a strong password so that no user can access another's account by logging on with a blank or simple password.

▶ **Set up each account with a screensaver and be sure the screensaver resumes to the Welcome screen**—To do this, right-click the desktop, click Personalize, and then click Screen Saver. Choose an item in the Screen Saver, and then activate the On Resume, Display Welcome Screen check box.

▶ **Lock your computer**—When you leave your desk for any length of time, be sure to lock your computer. Either select Start, Lock or press Windows Logo+L. This displays the Welcome screen, and no one else can use your computer without entering your password.

▶ **Use disk quotas**—To prevent users from taking up an inordinate amount of hard disk space (think MP3 downloads), set up disk quotas for each user. To enable quotas, select Start, Computer, right-click a hard drive, and then click Properties to display the disk's property sheet. Display the Quota tab, click Show Quota Settings, enter your credentials, and then activate the Enable Quota Management check box.

From Here

Here are a few other places in the both to turn to for information related to user accounts and other aspects of this chapter:

▶ For some logon tips and techniques, see the section in Chapter 2 titled "Useful Windows Vista Logon Strategies."

▶ To learn more about running a program under the Administrator account, see the section in Chapter 5 titled "Running a Program with the Administrator Account."

▶ For the details on group policies, see the section in Chapter 10 titled "Implementing Group Policies with Windows Vista."

▶ To learn how to work with the Registry, see Chapter 11, "Getting to Know the Windows Vista Registry."

▶ For information on sharing Windows Mail within a single user account, see the section in Chapter 19 titled "Working with Identities."

▶ You need to set up user accounts for the people with whom you want to share resources in a peer-to-peer network. For the details, see the section in Chapter 23 titled "Sharing Resources with the Network."