Chapter 3

# MASTERING ADMINISTRATION

## The Desktop Tech: A Modern-Day Hermes

If you research the Greek god Hermes, you come to appreciate the similarities to your desktop administrators. He was the chief messenger between humans (computer users) and gods (network administrators). He was the swiftest—nobody could get there faster than Hermes—and was later called Mercury in Roman mythology. He was also called the "most shrewd and resourceful" of the gods. Yes, all these descriptions aptly fit our desktop admins.

Although the Control Panel tools (discussed in Chapter 2, "Mastering the Control Panel") are a necessity to an admin. It's the Administrative Tools specifically and the System tools that are your greatest allies. We are going to discuss the tools and then some of the important considerations within Vista for desktop admins to keep in mind.

IN THIS CHAPTER

Depending on the situation, the desktop admin (also called the desktop tech, hardware tech, and so forth) can be the put in the role of network admin for a small network that uses all Vista machines instead of servers (or a mixed Vista–XP–Other) environment. The admin can be responsible for a department of systems that are connected to a larger network, in which case the responsibility would most likely include troubleshooting desktop issues, printer connectivity issues, hardware problems, and so forth.

The website www.infotech.com gives some clear job descriptions for the technology world.


The desktop technician's role is to provide a single point of contact for end users to receive support and maintenance within the organization's desktop computing environment. This includes installing, diagnosing, repairing, maintaining, and upgrading all PC hardware and equipment to ensure optimal workstation performance. This person will also troubleshoot problem areas (in person, by telephone, or via email) in a timely and accurate fashion and provide end user assistance where required.

Regardless of the role you play, be it a professional administrator or an at-home PC guru, you should be prepared to use the tools at your disposal. It's true that being part of a larger network can tie your hands on some of the resolution options. You might just have to call in the network systems admins. But the focus here is purely on what Vista has to offer. What can you, the Vista Master, do to administer the system? Well, you start by adding other user accounts to the network (small office or home).

# User Accounts

You can create new users in a couple of different ways. You can use the Computer Management MMC Console, or you can use the User Accounts applet from the Control Panel. The User Accounts applet found in the Windows Control Panel gives you most of what you need for adding users to a simple system. For a network situation, you should use Administrative Tools that can configure the Active Directory (the identity management database for Windows Servers).

## Literally Creating the Accounts

This part is simple. You can open the Control Panel, select the User Accounts and Family Safety option, and then select User Accounts. Or if you are working in Classic mode, you can just go directly to User Accounts from the panel, select Manage Another Account, and then select Create a New Account. You will have to choose a type of account: Standard User or Administrator. Standard User accounts are recommended if you are

going to have others using the machine who you do not want to provide permissions to because they might pose a security risk (inexperienced users or children). After the account is created, you can change the password for it, change the picture, and establish Parental Controls (which you learned about in the last chapter).


*Terri Stratton*
*Microsoft MVP*

One of first things I do (as I use classic mode and 'display as menu' on Computer, Control Panel, etc.) is to right-click the Start orb, select Properties, then Customize, and add Administrator Tools to both All Programs and the Start Menu.

A more advanced way to create an account is through your Administrative Tools, Computer Management (which opens the Computer Management MMC) console. You can also right-click Computer and select Manage to open this console. Using this method can give you a greater level of control over your accounts in that you can configure Group memberships, password settings, and profile/home directories all from a centralized location.

From here, you can expand Local Users and Groups, right-click the Users folder, and select New User (or select the Users folder and select New User from the Actions pane under More Actions).

Type in a username and full name—the description is optional (see Figure 3.1). Then enter a password and one of the following options to go with the account:

- **User Must Change Logon at Next Logon**—The first time the user logs on to the system, she is asked to provide her own personal password, as opposed to the one you've assigned.
- **User Cannot Change Password**—Forces the user to use the password you created.
- **Password Never Expires**—With this option, the user never has to worry about changing her password.
- **Account Is Disabled**—Makes it so that the account is temporarily inaccessible. This is a good option if a user account is going to go unused for an undetermined amount of time but you think the user might be coming back. You can disable

**TIP** If you want to delete a user account, you can do that from within the same User Accounts applet. When you attempt to delete the account, it asks you if you want to delete everything or if you want to have a copy of the user's Documents, Favorites, Music, Pictures, and Videos folders on your desktop. It will not copy email messages or other settings, but this is a great way to preserve the user's personal items or more easily move them over to another machine.

her account as a preventative security measure but not delete it until you know the account will never be used again. This frequently comes into play in corporate environments as employees come and go (and frequently come back again).

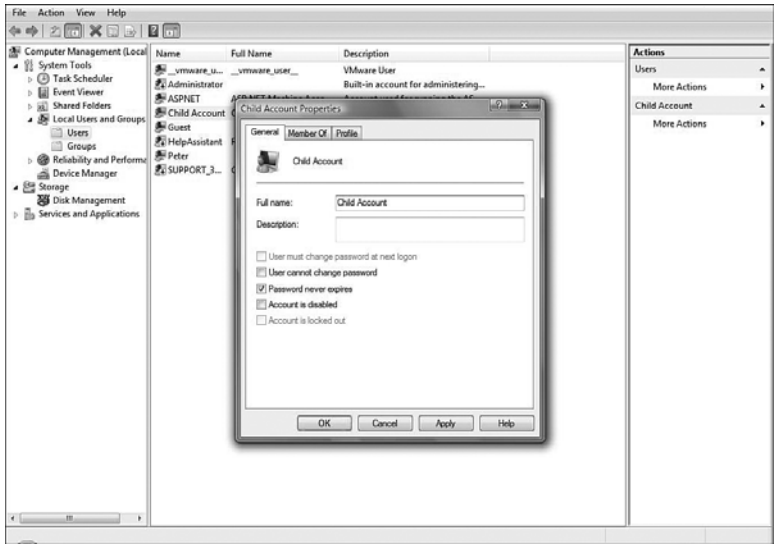


**FIGURE 3.1**

*Creating a new user account through the Computer Management Console.*

## Using Net User to Create Accounts

When I was in fourth grade, they taught us the programming language BASIC in an after-school program. We used simple command statements like these:

```
10 Print Hello
20 Goto 10
```

There's something oddly fun about seeing "Hello" scroll up and down the screen. Some of us just love the command prompt way of doing things. For many Windows gurus, they can just get things done more quickly via a command prompt, but I also have no doubt that for many vets it also goes back to those early days of BASIC and Commodore 64 programming. So, if you want to create a new user in Vista from the command prompt, you can use the `net user` command.

Start by opening a command prompt in elevated mode, as was discussed in Chapter 1, "General Tips and Tricks of the Masters." Then type **`net user /?`** to see your options. The `/?` tells Vista to list all the options you can associate with the `net user` command.

To try one example, type the following:

```
net user tim Ou812! /ADD
```

This creates a user named Tim with the password of Ou812!. To confirm this, open your User Accounts applet and see that this new account exists.

For more information on how to use the `net user` command see the Microsoft Knowledge Base article: http://support.microsoft.com/kb/251394. And there are other uses for the "net" command, you can find here: http://www.chicagotech.net/netcommand.htm

## Modifying Your User Accounts

Without going into a discussion of Active Directory and Vista, you have to know that modifying user accounts in this discussion involves the Vista-only angle. Obviously, Active Directory modification allows for more options, but the focus here is Vista.

From within the User Accounts applet, in addition to changing a user's password or picture, a sidebar is available from which you can choose one of the following:

- **Create a Password Reset Disk**—You'll need a floppy drive or a USB drive to start the process. The concept is simple: You are asked for your password and then that is stored on your disk as a `.psw` file. In the event you forget your password, you can log on with your disk. Keep in mind that anyone can use the disk to log on so this is something you don't want to leave around for others to get a hold of. This password is only for your local system logon. If you log on through a domain controller into an Active Directory domain at work and you forget your password, you will need your network admin to give you a new one.
- **Manage Your Network Passwords**—You can store passwords for networks or websites you visit through this option so Windows will log you on automatically when you visit those servers or sites. Just type in the computer name on the network or the URL and then enter your username and password. (Again, this is not for an AD domain, but it can be very helpful if you have a small peer-to-peer network with a member server and so forth.) The Vista Security Team (http://blogs.msdn.com/windowsvistasecurity/) also said:

> **CAUTION** It's very important to remember that a person might forget his password and that you as an admin can then reset it. However, if you do this, the user actually loses access to encrypted files, email messages that are encrypted, and stored passwords for servers or websites. This is another reason it's a good idea for users to use their password reset disks. When they use the password reset disks, they are changing their passwords and this doesn't harm their access to encrypted resources.


Stored User Names and Passwords in Windows Vista includes a Backup and Restore Wizard, which allows users to back up user names and passwords they have requested Windows to remember for them. This new functionality allows users to restore the user names and passwords on any Windows Vista system. Restoring user names and passwords from a backup file will replace any existing saved user names and passwords the user has on the system.

- **Manage Your File Encryption Certificates**—We will discuss encryption in Chapter 5, "Disk Configuration and Volume Tricks," but this option helps you manage smart card certificates or even personally created certificates for encryption. You can back them up in the event the certificate is lost as well.
- **Configure Advanced User Profile Properties**—Profiles are basically your likes and dislikes for the system to store and remember when you log on. So when you sit down and log on, you see the mountain background but when another person logs on, he sees something else. If you don't use a network and just work off your own system, you have all your profile information stored on the local system. But if you move around from machine to machine, rather than reconfiguring a local profile on each system, you can configure a roaming profile. This means the profile is stored on an accessible server and when you log on, your settings are brought down to your system from that server. So, you can move around all you want and you still see the mountain background. But, if you log on and the profile you have isn't available (say, the server is down for maintenance), you will still be able to log on with a locally cached profile.
- **Change My Environment Variables**—The most technical option of all in User Accounts is this one (shown in Figure 3.2). Environment variables tell your computer where to find certain types of information. You'll notice that there are user variables (for settings specific to users and their profiles) and system variables (which indicate locations of critical system resources). These variables can be edited or added to.

  One reason for doing this can come into play when creating a boot CD (as we

NOTE

There have been some changes in the way profiles work under Vista. Although roaming profiles solve one problem (that of users moving from one workstation to another), they cause others. For example, those profiles can become quite large and cause excessive logon times. Folder Redirection solves some of these problems because the profile data is separated from the user data. Another change is the location of the profiles. Previously stored under Documents and Settings, they are now stored under Users. They aren't nested so deeply as they were before and are structured more intuitively. For more information on the changes, do a search for the "Managing Roaming User Data Deployment Guide" from Microsoft. Type this into Google and you will be directed to a document for download.

discuss in Chapter 8, "System Recovery and Diagnostic Tricks"). Boot CD's generally use a variety of command line tools that are not located in the standard set of environment variable folders, so it's beneficial to edit the environment variables for the system so that when you want a tool, you do not need to navigate to the specific folder that holds that tool. You can type it from any folder location and the system knows where to look to find it.

These options have changed somewhat from the past and so it's good to note the changes listed in Table 3.1, which was posted on Jason Conger's blog at http://blogs.msterminalservices.org/conger/2006/09/12/profile-and-environment-variable-changes-in-vistalonghorn/. However, as Jason notes on his blog, it's important to bear in mind that these changes can cause problems with login scripts. Particularly scripts that have hard-coded paths.

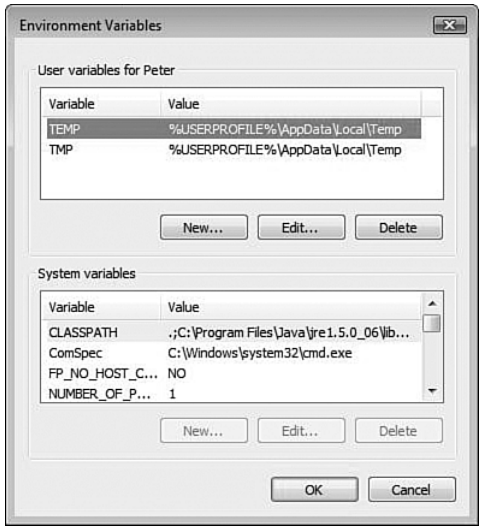


**FIGURE 3.2**

*Environment variable changes.*


To quickly access specific locations that have parameters set in the environment variables, you can go to the Start orb and type the variable into the search or Run command dialog box. For example, although Vista allows you to go directly to the user folder when you select the Start orb and see the username on the upper-right side, you could simply type `%userprofile%` in the Search pane and the folder structure for the user logged in displays. The same goes for any of the other variables.

To configure environment variables from a command prompt, you can use the **`setx`** command. Type **`setx /?`** to see a full list of parameters for its use.

**Table 3.1**—Changes in Environment Variables from Windows XP to Vista

| Before Vista | In Vista |
|---|---|
| ALLUSERSPROFILE=C:\Documents and Settings\All Users | ALLUSERSPROFILE=C:\ProgramData |
| APPDATA=C:\Documents and Settings\<username>\Application Data | APPDATA=C:\Users\<username>\AppData\Roaming |
| HOMEPATH=\Documents and Settings\<username> | HOMEPATH=\Users\<username> |
| TEMP=C:\DOCUME~1\<username>\LOCALS~1\Temp | TEMP=C:\Users\<username>\AppData\Local\Temp |
| TMP=C:\DOCUME~1\<username>\LOCALS~1\Temp | TMP=C:\Users\<username>\AppData\Local\Temp |
| USERPROFILE=C:\Documents and Settings\<username> | USERPROFILE=C:\Users\<username> |

## Additional Options from the Computer Management Console

Although the majority of your settings can be found in the User Accounts applet, you can configure more advanced settings from the Computer Management console (or create your own console by typing **mmc** from the Search pane and then adding the snap-in Local Users and Groups). You can double-click any user and add the user to different groups or go to the Profile tab. From here, you can configure the following for a user:

- **Profile Path**—Your local computer already has a local path for the profile. But if you want the profile to be stored elsewhere on a network drive, for roaming purposes, you can configure the Universal Naming Convention (UNC) path here. (UNC paths take the following form: \\servername\sharename\folder.)
- **Logon Script**—Enables you to type the location of the logon script. These scripts can be helpful in performing all sorts of tasks, such as mapping your network drives. You might not be a scripting guru and that's okay—you don't have to be. You can find plenty of configurable free scripts on the Internet. For example, check out Don Jones' site http://www.scriptinganswers.com to learn more about logon scripts and other forms of scripting as well.
- **Home Folder Local Path**—Even though users have a Documents folder, you might want to configure the location for another home folder for a user. This can be local or remote.

- **Home Folder Connect**—If the home folder is remote, you can configure a drive letter for the connection so the user sees the folder as a personal drive letter in which she can store documents. That folder, if located on a server that is backed up daily, lets your users feel safe about their data.


We found this great little tip about accessing a hidden user panel from Serdar Yegulalp on the SearchWinComputing.com site (you can read more from Serdar at www.thegline.com). He mentioned typing the following command from either an elevated command prompt or the Search pane:

```
control userpasswords2
```

This opens a User Account's dialog box from which you can manage group memberships and passwords. You can even click a button on the Advanced tab under Advanced User Management that opens another MMC console but one that includes only Local Users and Groups.

# Computer Management

Administrative Tools comes with a list of mini-apps to work with, but the Computer Management option provides a grouping of tools in one console. It may not be the super console you would like to have (which you can create if you like), but it is a decent toolset collection.

The Computer Management tool, shown in Figure 3.3, allows you to manage local or remote systems through one console. You can monitor system events, work with hard disks, manage performance, schedule tasks, and so on.

Under System Tools, the following are available:

- **Task Scheduler**—Create and manage common tasks that your computer will carry out either automatically, or at the times you specify.
- **Event Viewer**—Used to view logs about events associated with file and directory replication, DNS, security, and more.
- **Shared Folder**—Categories include: Shares—Used to create shares and list all system shares. Sessions—Any open session from the local computer or a remote computer is listed. Open Files—Files being used by users or other computers are listed.

TIP To create a super MMC console go to the Start orb and type **mmc** from the Search pane. Then select File, Add/Remove Snap-In and select all the Snap-Ins you like. When you're done, select File, Save As and select the location for your `.msc` file.

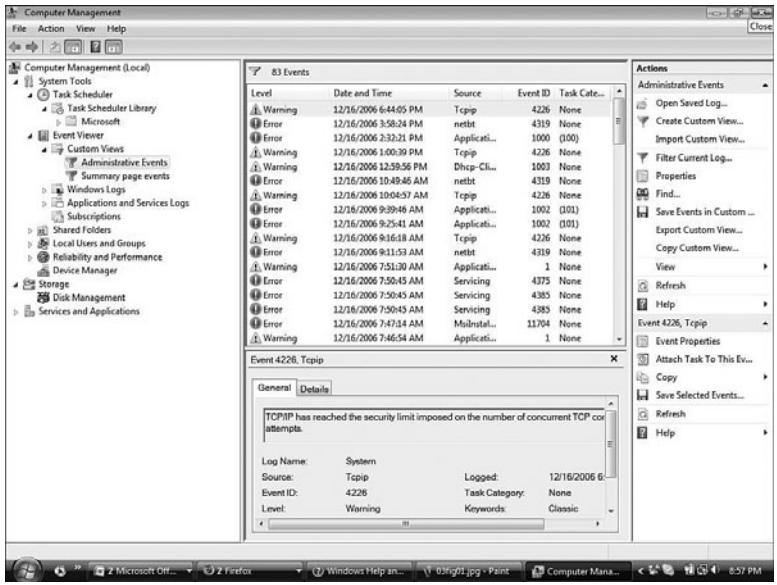


**FIGURE 3.3**

*The Computer Management console includes a bevy of tools.*

- **Local Users and Groups**—Used to make user and group accounts on the local computer.
- **Reliability and Performance**—Provides preconfigured diagnostics of your systems reliability and performance. You can also define your own counters to watch in real time or over a predefined period.
- **Device Manager**—Used to view all system resources.

Under Storage you'll find this option:

- **Disk Management**—Used to create, format, or delete simple, spanned, mirrored, striped, or RAID-5 volumes. Also provides information about the disk regarding the status and health.

Under Service and Applications are the following:

- **Services**—Lists all services (started or not) and the Startup Type (Automatic, Manual, or Disabled).
- **WMI Control**—Windows Management Instrumentation control allows monitoring and controlling system resources.

We've already discussed Local Users and Groups. Reliability and performance (in Chapter 8, "System Recovery and Diagnostic Tricks"), as well as disk management

(in Chapter 5), are discussed later, while Device Manager was discussed in Chapter 2. This section discusses Task Scheduler, Event Viewer, and Services.

## Task Scheduler

Vista really gives the Task Scheduler a much-needed overhaul. Now you can configure the Scheduler to perform tasks on a timed basis and to respond to situations that occur on a variety of levels. The response system can even restart a service that has failed or send an email to the admin when a certain event has occurred.

The Task Scheduler is integrated with Event Viewer now so that it can react to situations based on trackable events that occur. There is also a way to view the task history. You can see which tasks are running, have run, or are scheduled to run.

In addition, an entire Task Scheduler Library has preconfigured tasks with which you can work (see Figure 3.4).

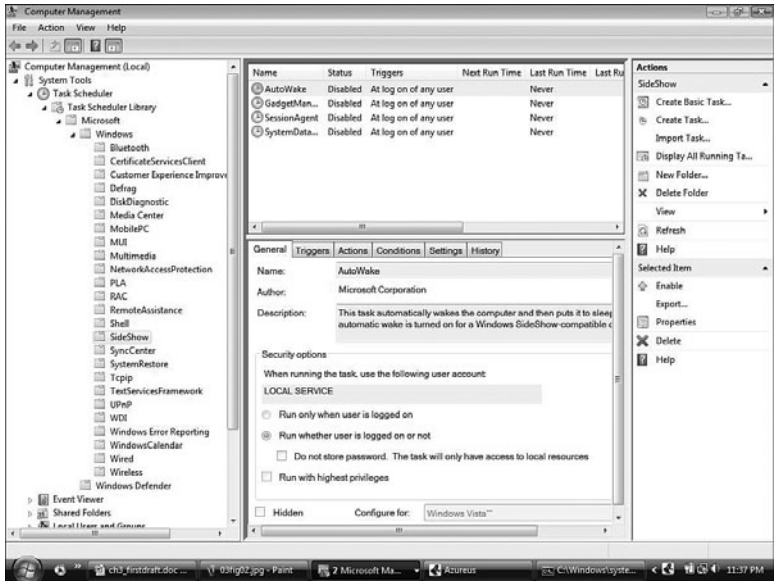


**FIGURE 3.4**

*The Task Scheduler has an entire library of options, or you can create your own using the basic options or the more advanced tabular dialog box.*

### Triggers and Actions

A *trigger* is what causes the task to run, and an *action* is what you have configured to occur in the event the trigger goes off. Some triggers are schedules you put into effect. For example, if you specify that every day at 1:00 p.m. a certain action should occur, the trigger is the scheduled time. But a trigger can also be when a user logs on, when the system starts up, when a specific event occurs, and so forth. An action is whatever task the system executes in response to the trigger. Actions can include running a program, sending an email, or even displaying a preconfigured message. There is a list of possible actions to take, including running scripts with the `cscript.exe` application, copying a file with Robocopy, starting and stopping services, shutting down the system, and a host of others.

#### Copying Files with Robocopy

Some (well, Tim Sneath in particular, but we agree with him) have called Robocopy (Robust Copy Utility) the coolest command-line tool in Vista. Many of us have used Robocopy for years because it was the only way we could copy large file structures. In the past we always had to get it from the Windows Resource Kit, but it's now in Vista for everyone to use.

Here are a couple of cool points about Robocopy: It has a whole bunch of switches (the original documentation was more than 30 pages long). Type in **`robocopy /?`** and watch the magic. There are really too many switches to get into here, so you'll have to research it a bit to see what it can do. I'm sure you'll find that it's quite flexible. For example, if a network link goes down during the copy, it doesn't shut down, it just waits. You can configure the wait time parameters. It's great for mirroring large file shares because it only copies files that have changed and you can throttle the traffic so you don't use up your entire connection when you are going over a slow link.

One thing to keep in mind, if you are backing up user folders, use the `/XJ` switch to exclude copying junctions.

### Scheduling a Task

You can do this in several ways. First, from the console, you can open the Actions pane and select Create Basic Task. This walks you through the following options:

- **Create a Basic Task**—Start with a name and description.
- **Trigger**—You can work from a schedule (daily, weekly, monthly, one time) where you set time parameters for the triggered event. You can also select When the Computer

Starts, When I Log On, or When a Specific Event Is Logged. In the case of the latter, you can select the Log, the Source, and even the Event ID that triggers the next step.

- **Action**—You can start a program (and choose which program that is), send an email (with the information for the email), or display a message (and write the message you want displayed).

> **TIP** The time settings relate to the time zone that the system is currently in. However, if you check the Universal box, the time zone connects to Coordinated Universal Time (UTC); this is a good way to have multiple computers across multiple time zones perform a task on the same time schedule.

- **Finish**—You can review your new task and tell it to open the properties of the task. When this happens, you can see a much more complicated tabbed view of a task. These options help you go beyond the basic task. You can create and manage your tasks in this way, or you can create a task from the more complicated tabs to start with.

To create a task that goes beyond what you can do when creating a Basic Task, select the Create Task option from the Action pane. This offers a dialog box with five tabs to configure your tasks. The tabs include the following:

- **General**—Enables you to configure the name and description of the task, under which user account it should run, and whether it should run only when that user is logged on or not.
- **Triggers**—Here you can schedule an extensive list of triggers, starting with the time triggers you can set up. If you change the Begin the Task options, the settings will. The most complex of the triggers involves Events.
- **Actions**—The actions you can perform are no different here from what they were from the basic settings. You can configure a program to run, send an email, or display a message: Or you can do all three if you like. That is the benefit to using the advanced tabbed task creator. You can configure different actions to occur from here.
- **Conditions**—This tab enables you to specify conditions to your task. For example, you may want certain tasks to run only if the system is idle. Other conditions might depend on whether the computer is running on AC power or battery power, or if it is or isn't connected to a specific network.
- **Settings**—Allows you to determine whether you can start the task manually, what to do if your task couldn't run on schedule, what to do in the event a task is running too long, and so on.

### Importing and Exporting Tasks

All of a task's properties (triggers, actions, conditions, settings) are held in XML files. You can export these XML files and import them on other systems.

Importing is quite simple; you can see the import option on the Action pane while working with the task manager. To see the export option, you must open the Task Scheduler Library folder. You can export the tasks you have created or export the preconfigured tasks within the library (although this would make sense only if you have configured them differently in some way). To export a task you select the task, right-click and choose to export. Choose the location for the `.xml` file that will be created. To import you can right-click any of the task folders and choose import task and then select the `.xml` file you want to import.

### The AT Scheduler, Command Prompt Options, and Scripting

The AT command is the tool that was historically used to schedule tasks through the command-line in previous versions of Windows. Call it nostalgia, but for some reason Microsoft hasn't removed the `at.exe` command from Vista even though it has replaced it with the `schtasks.exe` command. What does this mean? Well, if you have worked with the `AT` command for many years and are comfortable using it, you can still use it in Task Scheduler. All tasks created with the `at.exe` command must run on the same account, which you can configure through the AT Service Account Configuration option from the Actions pane.

But, if you want to work with the latest tool, the `schtasks.exe` command enables you to do many of the same operations on local or remote systems. You can create, delete, query, change, run, and end scheduled tasks. Type one of the following commands for help on using `schtasks.exe`:

```
schtasks /Create /?
schtasks /Run /?
schtasks /End /?
schtasks /Delete /?
schtasks /Change /?
```

Scripting the Task Scheduler has been made more fun now that you can go beyond `at.exe` and even `schtasks.exe`. With Vista, you can access the Task Scheduler API through scripts. Microsoft provides a nice article on this at http://www.microsoft.com/technet/scriptcenter/topics/vista/tasks1.mspx.

This article walks you through the beginning stages of scripting the task scheduler, and whoever wrote it is more than intelligent, but knows how to take dry-programming-speak and turn it into a fun article.

### Having Some Fun with the Task Scheduler

Fun? Are Vista Masters allowed to have fun? Well, in addition to saving the universe, we need to enjoy our work. Here are some fun things to try with your Task Scheduler:

- Need your religious or comedic fix in the morning? You can also set the task scheduler to start up an installed Daily Scripture program, or a set Bible reader, or if comedy is more your needed wake-me-up go to the Calvin and Hobbes site (or whatever comics make you happy).
- Need an expensive alarm clock? Set Task Scheduler to start up one of your music applications to open and play your favorite songs (or if you are a heavy sleeper, you can have a Godzilla MP3 set to go off, too). Want to live the movie *Groundhog Day*? Set the Sonny and Cher song "I've Got You Babe" to go off the same time every day?
- Make coffee and pick up your dry cleaning? Sorry, perhaps in the next version of Windows.


*Adam Pash*
*In, "Hack Attack: Using Windows Schedule Tasks," at Lifehacker.com*

Okay, so it's the middle of the night and you've defragged your hard drive and scanned for viruses. Before you get up and start working, though, you'd like that oh-so-fresh feeling that only a newly-rebooted Windows PC can offer. Try this bit of code for your Run line: `C:\WINDOWS\\system32\\shutdown.exe -r -t 01`

Note that because this command closes all applications and then reboots the system you might want to have a task run that restarts certain applications—perhaps your email client or an Office application you use every day.


*Adam Pash*
*"Hack Attack: Firefox extension packs," at Lifehacker.com*

No matter who you are, if you spend a lot of time on the Internet, chances are you have a set of pages that you visit to start the morning just like your morning paper. You're computer has been freshly restarted and is just sitting there, waiting for you to wake up—why not let it fetch your favorite pages so that your morning reading is ready and waiting for you. Set up a task to open Firefox just as you did above, then add all of the websites you'd like to visit following your run line separated by a space. The resulting line should look something like this: `C:\Program Files\\Mozilla Firefox\\firefox.exe" lifehacker.com del.icio.us/username nytimes.com wikipedia.org gmail.com`

## The Vista Event Viewer

We've been using Event Viewer for years, but most people check it only when there is a major problem. They see if they can quickly discover which service stopped or what caused the glitch; then they forget about it again until the next big problem. This is not truly taking advantage of the powerful technology at our fingertips. Although upon first look, Vista's Event Viewer can appear overwhelming, let's see if we can tame it a bit.

NOTE

For more tips on using the Task Scheduler or other tips, check out www.lifehacker.com. This site has one tip for running a vbs script that allows you to keep track of your weight each day in an Excel spreadsheet. The script is free to download along with a bunch of other free scripts you can use to clean up your hard drive and so forth. You can spend hours on this site looking at all the cool tools and articles.

The Event Viewer (shown in Figure 3.5) enables you to see more than the standard Windows logs (Application, System, and Security logs). Now there are Applications and Services logs, which include diagnostic logs, logs for specific applications within Vista, like your IE logs. In the past, you had to hunt to find logs for certain applications, but Microsoft has tried to bring them all together here.

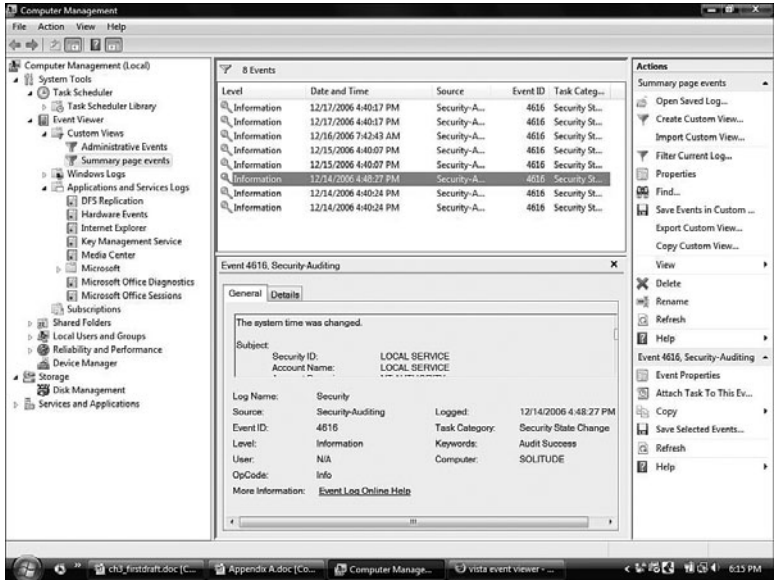


**FIGURE 3.5**

*The Vista Event Viewer is more robust, offering an Enterprise monitoring functionality.*

### Custom Views: More Than Filters

So many events come into the Event Viewer that it's almost impossible to track down the problem you are investigating without some form of filter. Views allow you to create filters that not only filter the events of one log, but also enable you to select multiple logs to view. To create a custom view, you select a log, open the Action pane, and select Create a Custom View, shown in Figure 3.6.

**TIP** We just discussed the Task Scheduler and how great it is with assigning events as triggers that require actions. Well, instead of memorizing the events you want so you can put them in Task Scheduler, you can find the event you want in the Event Viewer, right-click it, and select Attach Task to This Event (or you can find this option in the Action panel). This enables you to create a basic task that you can configure further from the Task Scheduler.

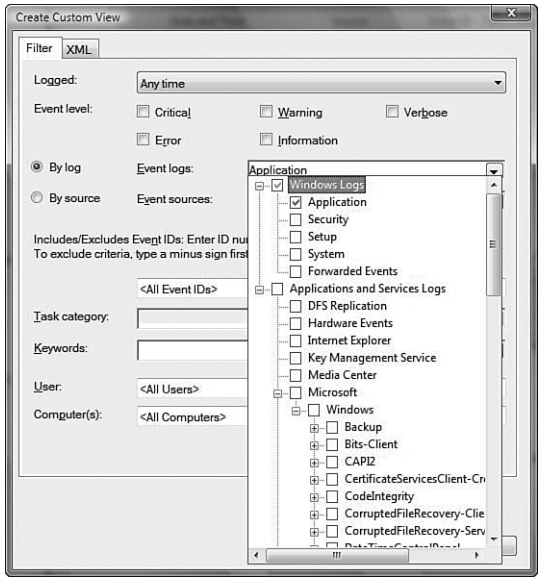


**FIGURE 3.6**

*Creating a custom view and choosing the logs included.*

From the Custom View dialog box, you can configure the following options:

- **Logged**—Enables you to provide a time frame for the events.
- **Event Level**—Critical, Warning, Error, Information, and Verbose.
- **By Log**—Select the Event log or logs from a checkbox hierarchy.
- **By Source**—Select from a source hierarchy, including applications and services.

- **Event IDs**—If you know the specific ID you are looking for, you can put it here or enter several IDs separated by commas.
- **Task Category and Keywords**—Select from the checkboxes that drop down. Filtering by keywords is a new feature we can all appreciate.
- **Users and Computers**—You can have the view look for specific users and can even filter through multiple computers.

## XML Event Viewer Details

XML is everywhere in Vista. Event Viewer is no exception. If you look at the properties of an event, you will be met with a scary-looking XML structure (shown in Figure 3.7). You can switch over to the Friendly View if that makes you feel better.

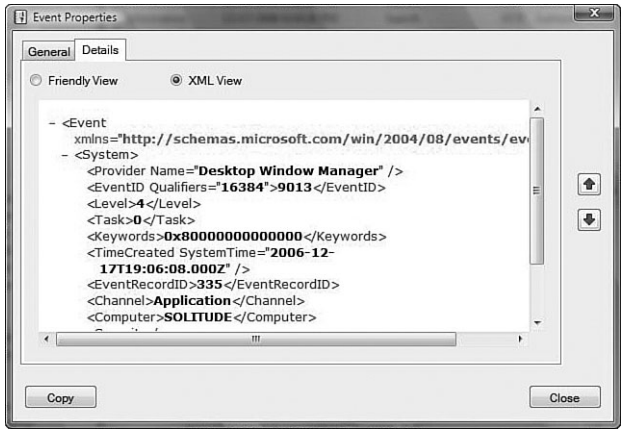


**FIGURE 3.7**

*XML is everywhere in Vista, including Event Viewer details.*

Why is the information stored as XML? It makes it easier for applications to take advantage of it for centralization and consolidation of the data. Other applications such as Microsoft Operations Manager (MOM) and Systems Management Server (SMS) (and others that are in the works) can take advantage of the XML open-sourced format of the data.

You can right-click any event and choose "Event Properties" to obtain more information. From the Properties, the General details provide the information you most need to troubleshoot that particular event, if the event indicates a problem with your system. You'll notice that you still have the ability to request help from Microsoft through the Event

Log Online Help option, which usually says something like, "Sorry, even though we created the program we have no how idea to help you…we're really, really sorry." Okay, so it doesn't say that, but it is frustrating much of the time.

> **TIP** Do you really want to know what the Event IDs are telling you in Event Viewer? Check out EventID.net. This is an online community of tips and tricks from other admins who are all seeking event enlightenment. At the time of this writing, close to 9,000 events existed in the Event ID database with about 500 event sources and about 15,000 comments provided by almost 3,000 contributors. It's worth checking out if you have difficulty understanding an event.

### Subscriptions

You can collect logs from remote systems and save them onto your local system through subscriptions. For this to work, you have to configure the collector (the system that collects the events) and the remote source systems.

To configure the source systems, type the following command from an elevated command prompt

```
winrm quickconfig
```

To configure the collector computer, type the following command from an elevated command prompt

```
wecutil qc
```

On the source computers you will need to add the computer account of the collector to the local Administrators group on each computer.

After the systems are configured to forward and collect events, you can create new subscriptions through the Event Viewer. There are more details you might need to consider depending on your environment, such as opening ports for your firewall to allow the event management exception and so forth. Going through the Help information from the Event Viewer offers a great deal of information on how-to advice and troubleshooting problems.

## Services and the SC.exe Command

Services are the underlying core OS features that handle any number of things on your system, from web services, to print services, and so forth. You've no doubt seen the services console before in XP or Windows 2000 because it has been around a long time.

The services structure hasn't changed much in Vista. You might notice a few more services in Vista. You now have the option to turn off some services to reserve system resources. But from within Service, you can do the following:

- Stop, start, pause, resume, or disable a service. You can also see the description of what each service does and which other services rely on it to work.
- Configure recovery actions in the event of a service failure (like restarting the service).
- Configure a service to run under the security context of a user account that is different from the logged-on user or the computer account.

NOTE If you enable or disable a service and your computer cannot start up, try starting the system in Safe Mode. Safe Mode is preconfigured with core services to start regardless of whatever settings you might have configured. Once in Safe Mode, you can make the changes to put the service back on that you accidentally shut off.

- Configure hardware profiles that use different services enabled or disabled.
- Export your services information to a `.txt` or `.csv` file.
- Monitor the status of each service.

You can use the `sc.exe` command to communicate and configure the Service Control Manager and services. You can also use the `net start` or `net stop` command to stop and start services, but SC is much more powerful.

An example of the **`sc.exe`** command is the following:

```
sc config <service name> start=<mode>
```

You can start with the following modes:

- auto—A service automatically started at boot, regardless of a user logging on or not
- boot—A device driver loaded by the boot loader
- demand—The default, a service that is manually started
- disabled—A service that is prevented from starting
- system—Started during kernel initialization

For more information on SC, type **`sc.exe /?`** from a command prompt.

# Sharing System Resources

We discuss networking in Chapter 7, "Master Vista Networking," and NTFS permissions in Chapter 5, "Disk Configuration and Volume Tricks," but here we want to talk about the simple concept of sharing. You have files, other networked users want access to those files, and sharing is the key. How is it done, how can you monitor what is being shared, and who is accessing it on your system?

## Sharing Files Through the Public Folder

The Public Folder (in XP called the Shared Documents folders) is the convenient and easy way to share files. Putting things in the public folder allows anyone who can access your computer to see and use the files as well as anyone who has been granted access to the files remotely via the network. There is only one set of public folders per computer, so all users on the computer add things to the same location.

To see the public folder, select the Start orb and then click Documents. You'll see a folder called Public in the Favorite Links pane. When you open it, you can see that other folders have already been created to make this easier: Public Documents, Public Music, Public Pictures, and so forth. All you have to do is copy or move the files over that you want to share to these locations.

NOTE

It's good to note, for novice sharers out there, that you cannot share individual files, only folders and all the files those folders contain. Sharing a folder means allowing access to that folder by users across the network. You can configure the level of access users can have through that network share, too. But keep in mind that you don't want to share everything you have, especially if you are working off a wireless network with no security settings (as many people are these days) because you are just inviting strangers into your computer.

Be careful about your sharing. Oh…and lock down your wireless network, too. We will talk more about this in Chapter 7, "Master Vista Networking."

Anyone with a username and password on your computer can sit down and access these folders, but you can determine how people across a network connection can (or cannot) access them.

If you want to make sure a person has a username and password on your system to access those folders, open the Network and Sharing Center (click Start, Network and click the Network and Sharing Center button on the Command bar). Look for the arrow next to Password-protected Sharing and then turn it on or off. Make sure, too, that the Public folder sharing is on. You can alter the permissions people have in accessing the Public folder by selecting the Public Folder Sharing option and then selecting one of the following options:

- Turn On Sharing so Anyone with Network Access Can Open Files
- Turn On Sharing so Anyone with Network Access Can Open, Change, and Create Files
- Turn Off Sharing (people logged on to this computer can still access this folder)

One thing to take note of is that this method of sharing doesn't allow you to structure permissions on a per-user basis. If individuals can access the Public folder, then they all have the same set of permissions that you apply. If you want to give different users

different permissions, or if you don't want two copies of files on your system one in your real folder and one in the Public folder), you might want to share out a different folder altogether on your system.

## Sharing Any Folder

You can right-click a folder and select Share. By default, this turns off the File Sharing Wizard. You can choose to share with users who are configured on the system with user accounts, or you can just allow everyone to access the folder through the share. This means users on other systems will be able to access the share even if they don't have an account on your machine.

If you don't like the wizard and prefer to share folders manually, you can turn off the wizard. Open the Control Panel and select Folder Options. Select the View tab and scroll down to the Use Sharing Wizard (Recommended) checkbox and deselect the box. Now, when you right-click a folder and select Share, you will be taken to the Sharing tab under the folder's properties. You will also see that the Share option is grayed out for the basic sharing. Instead you have to use the Advanced Sharing options (see Figure 3.8).

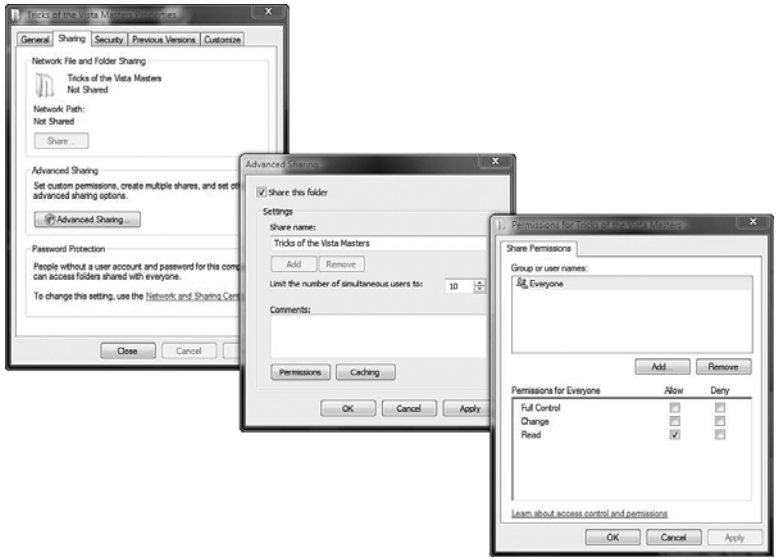


**FIGURE 3.8**

*Configuring the Advanced Share Permission settings.*

You might notice that you can also determine the number of users who can access the shared folder at any given time. The default setting is 10. You can control this further. If you know for a certainty that you only have 1 other person, for example, that will access the share, you can lower this to 1, and this will prevent others from accessing (or trying to access the share).

> **TIP** After you configure a shared folder, you can go back and click the Add button to share it again! Why would you want to do that? Well, you can configure a share with different names AND different permission sets.

The permissions you see aren't all that complicated to understand. You have Full Control (Allow or Deny), Change (Allow or Deny), and Read (Allow or Deny).

If we broke these down into smaller explanations, you would have the following:

- **Read**—Allows you to read a file (meaning read, listen to, view, watch, and so on with that file) and execute the file (if it is a program)
- **Change**—Allows you to read and execute the file, but it also allows you to write to the file (that is, open a Word document and make changes) or delete the file
- **Full Control**—Allows you to read, write, execute, and delete the file; plus you can take ownership of the file if you want and change the permissions of the file

Allow/Deny is an interesting dilemma. If you, as a user or a group you belong in, is assigned Deny in any way, shape, or form, on the object (printer, folder, drive share, and so forth), the Deny permissions are stronger than any of your Allow permissions.

To illustrate, let's look at an example of a shared folder. By default, everyone (which includes you) is given Full Control to access that folder through the share. However, you are part of a specific group that has been denied the ability to Read the folder. So this means that through the share, you won't even be able to open the folder to look inside. However, you could change these permissions for the group you're in because you have that ability through the Full Control set of permissions. After changing the permissions, you could then enter the folder.

If you think this is complicated, wait until we throw NTFS permissions into the mix.

Other ways you can share a folder are covered in the following sections.

### Shared Folders in Computer Management

From within Computer Management, you have the Shared Folders options. You can right-click the Shares folder and select New Share. Regardless of your folder options, this turns off the Create a Shared Folder Wizard.

From within Computer Management, you can do a couple of great things with Sharing. If you select the Shares folder, you can see all the folders and drive letters (even hidden ones) that are shared out on the system (see Figure 3.9). From here, you can right-click any share and choose not to continue sharing that folder. You can also go into the Properties of the share and alter the configuration, including the Share and NTFS permission settings.

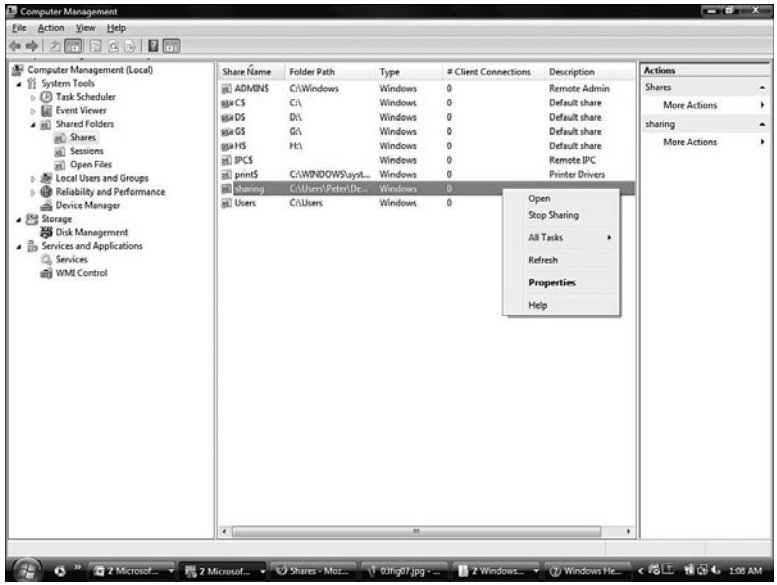


**FIGURE 3.9**

*We are back in Computer Management, this time looking at the Shared Folders options.*

If you select Sessions, you can see the users connected to your shares, which computers they are on, how long they have been connected, and so on. From here, you can right-click any user connected in a session and close the session.

You can also select the Open Files folder to see which files are being viewed, and you can right-click any file and close it. You should notify a user before you do this because otherwise the work they are performing on the file might be lost.

### Creating a Hidden Folder Share Is $

Why would you want to hide a share? Dorin Dehelean explains the reason to `http://www.windowsitpro.com` by saying:


To improve security on a Windows-based network, append a dollar sign ($) to your share names to hide shares from users. When you use this step in conjunction with tight NTFS and share permissions, you reduce incidental attempts by unauthorized users to click folders they shouldn't open. If users can't see the folders, they won't try to see what the folders contain. For authorized users, you can use a logon script to map the hidden share to a drive letter. Thus, only users who are authorized to access the folders will know the folders exist. Only technically savvy unauthorized users who know the exact path to the share can reach the restricted folders—and NTFS or share permissions will still deny these users access.

For someone to connect to those hidden shares, he must know they exist and then type in the share name correctly when he maps to that share.

### Connecting to Shares

You can view shares over the network by opening the Network window and viewing which systems exist that have shared folders to which you can connect. This is certainly the easiest way. Or, you can connect to a system using a mapped network drive.

A mapped network drive is basically a configuration in which you select a drive letter and type in a universal naming convention (UNC) path to the resource with which you are looking to connect. It sounds complicated—and it can be.

Right-click Computer or Network and select Map Network Drive to see the options. Or, from within Computer, you can select the option to Map Network Drive. When you select the option, you see the dialog box in Figure 3.10.

To map the drive, you select an available drive letter and then select the path. The path is `\\servername\sharename\<path>`. So, if you wanted to connect to a computer named Solitude to a share named Sharing, you would type `\\solitude\sharing`. You could also click the Browse button to see which shares are available, but you won't see hidden shares. To connect to those, you have to enter the share name with a `$` at the end.

You can also choose to reconnect at logon so that you will reconnect each time to that share and will not have map the drive each time.

Keep in mind that you can also connect to the server by using an IP address. So, you can also type **`\\serveripaddress\sharename`**.

**NOTE** Keep in mind that Network Discovery must be enabled in your "Network and Sharing Center" in order to use network mapping. If you aren't able to map to a shared out folder on another system, and you know the permissions are set properly, check to make sure that system has Network Discovery turned on.

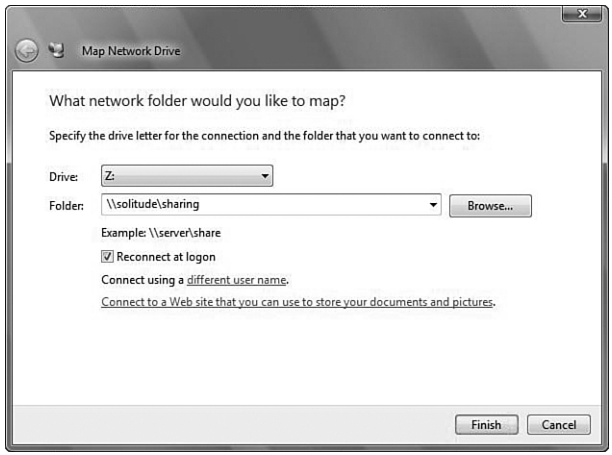


**FIGURE 3.10**

*Mapping a network drive.*

To map a drive from a command prompt, you use the `NET USE` command by typing the following:

```
NET USE <drive>: \\<server>\<share>\<path>
```

# The System Window

Want to configure your workgroup or network? Or configure Remote Assistance or Remote Desktop? Need protection? If so, you need to go see the Godfather, also called System.

You can find System in the Control Panel. Or you can right-click Computer from the Start menu and select Properties. You'll start off with a new graphical screen that gives you some basic information: the version of Windows, your Windows Experience Index (which we discuss later), your computer name workgroup/domain name, and the Activation options (see Figure 3.11).

**NOTE** There are a couple of cool things to keep in mind with `net use`. You can also use the IP address of the machine for the server. Or you can use a fully qualified DNS name (such as webserver.company.com). Instead of choosing a drive letter, if you just type an asterisk (*), `net use` just picks one for you from the available options. Finally, you can include more than the share name. You can include the folder itself so that in your scripts, if you use `net use`, you don't have to just connect people to a share—you can put them into a specific folder if you want.

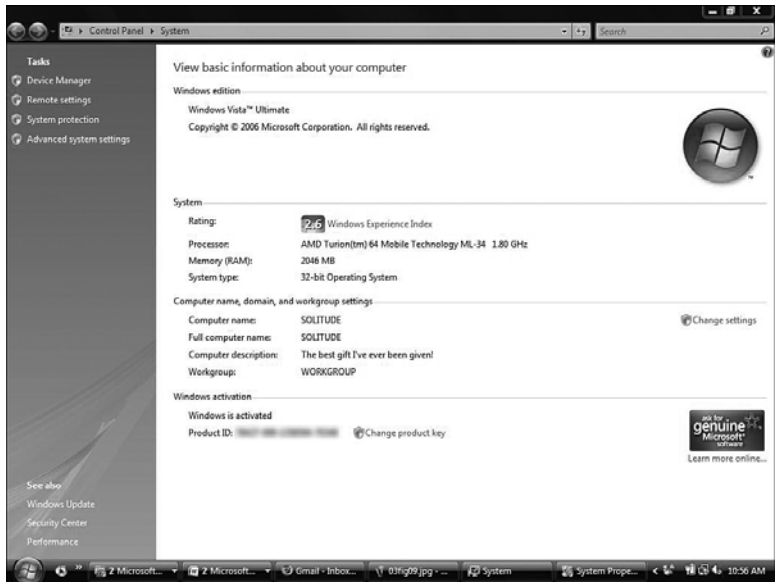


**FIGURE 3.11**

*Your initial System screen, before you get to any of the good stuff.*

On the left is a list of tasks. Click the Advanced System Settings link to see the System Properties, which includes five tabs. Let's discuss each one.

## Computer Name

On the Computer Name tab, you can change the description for your computer. If you want to join a domain (or workgroup), you can select the Network ID button, which starts an easy-to-use wizard that guides you through the process. If you don't need or want help, you can select the Change button and answer the questions for switching between a domain and a workgroup.

To join a domain, you must have a domain controller available (logically) and have a user account on the domain with the capability to join systems to that domain. Interestingly, if you are connected to a domain, you must still have those credentials to un-join and go back to a workgroup. This prevents users from removing themselves from the domain without permission.

**TIP** The fastest way to open System is to hold down your Windows Key and then hold down the Pause key (or on some systems the Pause/Break key).

From the Change options, you can also change your computer name. Or you can configure a DNS suffix for the system (which you don't have to worry about unless you are part of a domain, and even then it's rare) or change the NetBIOS name for the computer.

## Hardware

The Hardware tab contains two options. The first is Device Manager, which we talked about in Chapter 2. The second is Windows Update Driver Settings.

If you select the Windows Update Driver Settings button, you will see the Windows Update Driver Settings dialog box and be presented with three options:

- Check for Drivers Automatically (Recommended)
- Ask Me Each Time I Connect a New Device before Checking for Drivers
- Never Check for Drivers when I Connect a Device

## Advanced

The Advanced tab gives you options to enhance your system's performance. For an admin, this is like a candy store of options. There are three sections to focus on in this window: Performance, User Profiles, and Startup and Recovery. Each has a Settings button you can click to modify your system's advanced system properties.

### Performance

When you click the Settings button for Performance, you'll find that there are three tabs with which you can work:

- **Visual Effects**—Choose to configure Vista for best appearance (which turns on all options) or performance (which turns off all options). Or you can go through all the options and manually make adjustments that will give you what you need. If your system is acting sluggish, your best option is to turn off some of these and see whether performance improves, without losing all your favorite effects.
- **Advanced**—You can change the Processor Scheduling to either Programs or Background Services. And you can configure your Virtual Memory.

  The options under Processor Scheduling relate to how your processor (which can only handle so much work at a time) divides its attention among multiple applications. If you leave the setting to Programs, the processor devotes the majority of its time to the program running in the foreground (that's whatever program you are currently working in). If you select Background Services, the processor devotes time equally to all applications.

- **Data Execution Prevention (DEP)**—This is the final tab under Performance. DEP monitors your system to ensure that programs use system memory properly. Although DEP is a software-based protection feature, some processors are also DEP enabled for hardware protection. The two options you can configure are Turn On DEP for Essential Windows Programs and Services Only and Turn On DEP for All Programs and Services Except Those I Select. Then you can configure which programs you don't need monitored.

TIP If you or your users complain that programs are running too slowly, you should ensure that this is on Programs so that the active program gets the majority of the processor's attention. However, if you or your users frequently run background processes, such as macros, you should give all applications equal time slices (which are called *quanta*) by enabling the Background Services option.

NOTE DEP has been known to cause problems with some older applications. If you run into a conflict and trust the application that causes it, you should turn on DEP for all programs and configure it so that it doesn't check the applications you want to be able to run.

## Understanding Virtual Memory

Virtual memory is something you generally don't have to worry about. If you open this setting, you can see that the option at the top makes you feel good inside—it tells Vista to handle it without your help. However, any true Vista Master knows what it is and how to configure it if needed. Ronald Barrett, the Senior Network Administrator for ERE Accounting in Manhattan, says:


Imagine your computer is like an office. Your hard disk is your file cabinet and your desktop is your, well…desktop. Every time you want a file or folder, you have to get up and go to the file cabinet. That slows down your workday. But, say you have a set of folders on your desktop that can hold the latest work—that is your RAM. In addition, you have a little spot right in front of you for the stuff you need immediately—that's your cache. You can start to see how it all comes together for your workflow. Your virtual memory involves a situation in which your computer is working hard, moving files back and forth between the RAM, but finds that it needs more space. There is no more RAM and it doesn't want to put it back in the large file cabinet of a hard disk; what can it do? Instead, a pagefile is created (also called a *swap file*). This is on the hard disk (back in the file cabinet), but it's really an extension of the RAM itself so that RAM can quickly access what it needs. So, even though it's on the hard drive, it's called virtual memory. Got all that?

Now, even though we said you can let Microsoft handle it, the fact is that there are some best practices Vista knows but ignores.

If you have multiple drives, you can divide the pagefile between all the drives you have (drives, not partitions). The more drives, the better. You should also try to get the pagefile off your system file drive (`c:` drive). If you have any drives that are fault tolerant (discussed later), you should keep the pagefile off these drives.

Microsoft generally sets the minimum size of the pagefile to the amount of RAM you have plus 300MB. The recommended size is 1.5 times the amount of RAM. You can increase beyond that if you want. Generally, though, it's best to go with the recommended and just split it up amongst your drives and get it off that system drive (but not on fault-tolerant drives).

### User Profiles

Explained earlier as your likes and dislikes for your desktop, you can use the user Profiles tab to delete profiles on the system from here. You can also copy profiles to give to other user accounts and configure roaming or local user profiles if you have a profile configured as roaming.

### Startup and Recovery

The Startup and Recovery options, shown in Figure 3.12, haven't changed from Windows XP.

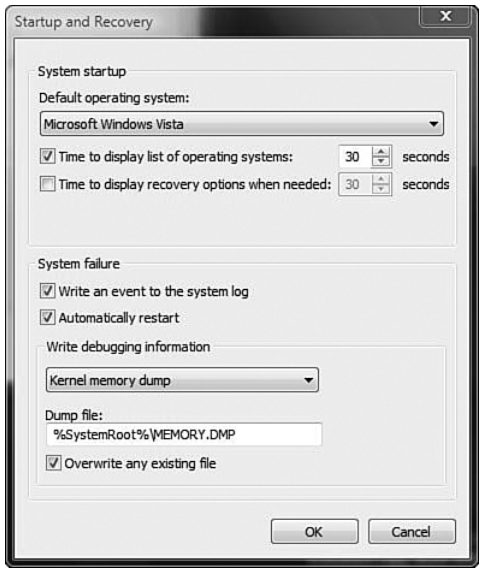


**FIGURE 3.12**

*Startup and Recovery options.*

The System Startup section lets you select the OS to which to boot up (only important if you have multiple OSes on the same machine) along with a boot time. You can also configure startup to automatically show the recovery options for a period of time (instead of pressing F8) during bootup.

The recovery options are for those special "blue screen of death" moments that occur in all our lives. (Although, hopefully, their frequency will be much less in Vista.) Sometimes you want the system to reboot and get it over with; other times you want to see the blue screen before the system reboots so you can see what's happening.


*Terri Stratton*
*Microsoft MVP*

One of the first things most techs and support personnel that I deal with advise is that users turn off the 'automatic reboot' feature so that they can see the problem without having to use the Event Viewer, which may or may not give the same information. This is especially true now that so many errors can recover without a reboot (although not a blue screen).

In addition, you can configure the extent of the memory dump that occurs, the location of the dump file, and so on. Here are the types of memory dumps you can configure, besides none, which is self-explanatory:

- **Complete Memory Dump**—Records the entire contents of memory. Basically, during the crash, your RAM is copied over to the pagefile, which is then saved as the `memory.dmp` file during the reboot process.
- **Kernal Memory Dump**—Records only kernel memory, driver memory, and HAL memory (which should suffice to know what crashed the system).
- **Small Memory Dump (64KB)**—Lists the stop message and parameters, loaded drivers, processor context, and running thread information.

To understand what has actually occurred, you need to analyze the dump file. You can download the latest Windows debugging tools from http://www.microsoft.com/whdc/devtools/debugging/default.mspx. In addition to the tools, plenty of documentation is provided.

## System Protection

The System Protection feature lets you create restore points so you can quickly jump back to a point in time when your system was working perfectly. This feature affects only the system; it does not undo files, photos, or other items you have created on your system.

So, for example, if you've installed a program or new driver and the system cannot handle it, you can try to uninstall the problem. If that doesn't work, you can use a restore point to jump back.

System Restore is an option from All Programs, Accessories, System Tools. You can run this wizard when you want to restore a previously created restore point. But, you create the points from your System Properties. Restore points are automatically created every day and when you install new applications and drivers. You can also go into your System Properties, open the System Protection tab, and select the Create button to take a snapshot of the system as it is at that moment.

Restore points require at least 300MB of space on any given hard disk where they are turned on.

**TIP** You can configure the times for System Restore points by going into the Task Scheduler, looking through the Task Scheduler Library, under Microsoft, Windows, SystemRestore. Under the SR task, you can see that the task provides two triggers, one for a time schedule (default is 12:00 a.m.) and one for system startup.

## Remote

Remote is where the settings for Remote Assistance and Remote Desktop reside. The Remote Assistance feature is more helpful than most people give it credit for. I cannot count how many times family members have called asking for assistance and I just had them send me an invitation so I could see what they are doing and either take over or walk them through the changes.

The settings are simple. You can set Remote Assistance to make connections that allow desktop control. You can also determine the length of time for the invitations to be valid. To invite others to use your system or accept invitations, go to the Windows Help and Support dialog box and look for the Windows Remote Assistance options.

Remote Desktop enables you to connect to another computer as if you were sitting at it. So, for example, you can access your work computer from home (if your work computer is on, configured to use Remote Desktop, and the Firewall allows the connections).

To connect to a system, you use the Remote Desktop Connection tool under Programs, Accessories. You can configure quite a bit, including the display settings and the use of resources.

**TIP** In Vista, the Remote Desktop can span multiple monitors. You must type **`mstsc /span`** at a command prompt to accomplish this. To toggle in and out of full-screen spanned mode, you press Ctrl+Alt+Break.

# More Useful Tools

We cannot pick apart every last little feature. It's just not practical or necessary when you have an Internet filled with article after article that will round out your knowledge on any one of these tools. The key is to know they exist and to know what they do—a true master takes what she's been given and adds to it. Here are some of the other tools you can use to help you administrate:

- **Data Sources (ODBC)**—Uses Open Database Connectivity to move your data from one type of database to another. So, for example, you can move data that was created on FileMaker Pro into an Excel format.
- **Defragmenter**—Found under the Accessories, System Tools, the defragmenter is no longer a graphical tool that you can watch move your data blocks around. But you can and should still schedule it, using either the tool or the Task Scheduler. It is set up by Task Scheduler to automatically defragment the drive once a week at 1:00 am, but if you know the system isn't on at that time then you will want to change the time.
- **Disk Cleanup**—Lets you free up disk space by searching through your folders for unnecessary or unused files. One great example of an unused file is the hibernation file. You can delete it from here (usually the size of your installed RAM).
- **Print Management**—Manages printers and print servers on a network.

Other tools such as the Memory Diagnostics Tool and the Reliability and Performance Monitor are addressed in chapters to come.

The following are some other resources an admin should know about and have in her utility belt:

- **Windows Vista Resource Kit**—Resource Kits are must-haves for any serious admin. These are sets of command-line tools that simplify the managing of Windows through a command prompt. The Windows 2003 Resource Kit is a free download that works on a variety of Windows systems and contains close to 200 tools. The Vista Kit can be purchased and includes a book and CD. Microsoft has a site dedicated to Resource Kit information: http://www.microsoft.com/windows/reskits/default.asp.
- **Sysinternals**—Mark Russinovich's incredible site of free tools has not been phased out now that he has moved into the Microsoft world; they have just been moved to this new location: http://www.microsoft.com/technet/sysinternals/default.mspx. Some tools to look out for are PageDefrag, Process Explorer, AutoRuns, BGInfo, and a bevy of others.
- **Adminpak (Windows Server 2003 Service Pack 1 Administration Tools Pack or Windows Server 2003 R2 Administration Tools Pack)**—These are free tools you can install on your Vista desktop if you plan on administering servers on your network. You

might have some difficulty running these to start with, but you just need to register the DLLs for the tools. An article at http://4sysops.com explains how to install the pack on Vista.

- **4SysOps.com**—It's not a collection of tools, but a website that is great for system admins to keep up-to-date on the latest and greatest tools and how to use them.
- **Microsoft BDD 2007 (Business Desktop Deployment)**—BDD 2007 contains important deployment tools for Vista, such as ImageX, WSIM (Windows System Image Manager), and WDS (Windows Deployment Services). You can download it at Microsoft Connect.