*Mastering Microsoft® Windows® 7 Administration*
by William Panek and Tylor Wentworth

# Chapter 8

# Configuring Users and Groups

One of the most fundamental tasks in network management is creating user and group accounts. Without a user account, a user cannot log on to a computer, server, or network.

When users log on, they supply a username and password. Then their user accounts are validated by a security mechanism. In Windows 7, users can log on to a computer locally, or they can log on through Active Directory.

When you first create users, you assign them usernames, passwords, and password settings. After a user is created, you can change these settings and select other options for that user through the User Accounts utility in Control Panel.

Group accounts are used to ease network administration by grouping together users who have similar permission requirements. Groups are an important part of network management. Many administrators are able to accomplish the majority of their management tasks through the use of groups; they rarely assign permissions to individual users. Windows 7 includes built-in local groups, such as Administrators and Backup Operators. These groups already have all the permissions needed to accomplish specific tasks. Windows 7 also uses default special groups, which are managed by the system. Users become members of special groups based on their requirements for computer and network access.

You create and manage local groups through the Local Users and Groups utility. With this utility, you can add groups, change group membership, rename groups, and delete groups.

In this chapter, you'll learn how to:

- Understand user account types
- Create accounts
- Configure accounts
- Understand local groups

## Understanding Windows 7 User Accounts

When you install Windows 7, several user accounts are created automatically. You can then create new user accounts. As you already know, these accounts allow users to access resources.

On Windows 7 computers, you can create local user accounts. If your network has a Windows Server 2008, Windows Server 2003, or Windows Server 2000 domain controller, your network can have domain user accounts as well.

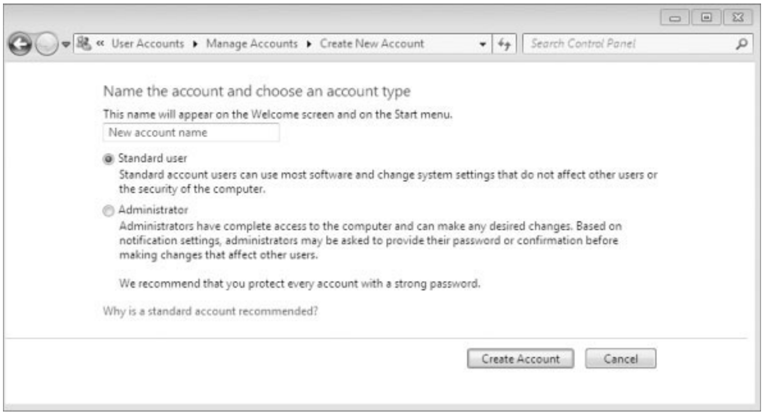
One of the features included with Windows 7 is User Account Control (UAC). UAC provides an additional level of security by limiting the level of access that users have when performing normal, everyday tasks. When needed, users can gain elevated access for specific administrative tasks.

In the following sections, you will learn about the default user accounts that are created by Windows 7 and the difference between local and domain user accounts.

## Account Types

Windows 7 supports two basic types of user accounts: Administrator and Standard User, as shown in Figure 8.1. Each one of these accounts has a specific purpose:

**FIGURE 8.1**
User Types screen



Name the account and choose an account type

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

New account name

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

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

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

Why is a standard account recommended?

**Administrator** The Administrator account provides unrestricted access to performing administrative tasks. As a result, Administrator accounts should be used only for performing administrative tasks and should not be used for normal computing tasks.

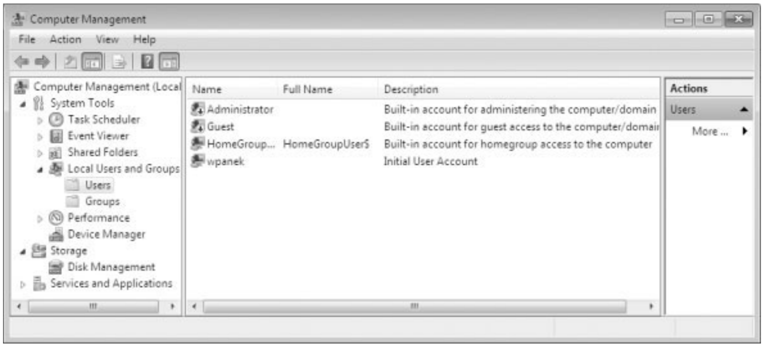
Only Administrator accounts can change the Registry. This is important to know because when you install most software onto a Windows 7 machine, the Registry gets changed. This is why you need administrator rights to install most software.

**Standard User** You should apply the Standard User account for every user of the computer. Standard User accounts can perform most day-to-day tasks, such as running Microsoft Word, accessing e-mail, using Internet Explorer, and so on. Running as a Standard User increases security by limiting the possibility of a virus or other malicious code from infecting the computer and making systemwide changes, because Standard User accounts are unable to make systemwide changes.

When you install Windows 7, by default premade accounts called built-in accounts are established. Let's look at these account types.

## Built-in Accounts

Built-in accounts are accounts that are created at the time you install the Windows 7 operating system. Windows 7, when installed into a workgroup environment, has four user accounts, as shown in Figure 8.2:



| Name | Full Name | Description |
|---|---|---|
| Administrator | | Built-in account for administering the computer/domain |
| Guest | | Built-in account for guest access to the computer/domai |
| HomeGroup... | HomeGroupUser$ | Built-in account for homegroup access to the computer |
| wpanek | | Initial User Account |

**FIGURE 8.2**
Four default accounts

**Administrator** The Administrator account is a special account that has full control over the computer. The Administrator account can perform all tasks, such as creating users and groups, managing the file system, and setting up printing. Note that the Administrator account is disabled by default.

**Guest** The Guest account allows users to access the computer even if they do not have a unique username and password. Because of the inherent security risks associated with this type of user, the Guest account is disabled by default. When this account is enabled, it is usually given limited privileges.

**HomeGroup User** The HomeGroup user is created by default to allow this machine to connect to other machines within the same HomeGroup network. This account is enabled by default.

**Initial User** The initial user account uses the name of the registered user. By default, the initial user is a member of the Administrators group.

### ADMINISTRATOR ACCOUNT

By default, the name Administrator is given to a user account that is a member of the Administrators group. However, in Windows 7 this user account is disabled by default. You can increase the computer's security by leaving this account disabled and assigning other members to the Administrators group. This way, a malicious user is unable to log on to the computer using the Administrator user account.

These users are considered local users and their permissions are contained to the Windows 7 machine. You can also have users logging into the Windows 7 computer that are considered domain users. Let's look at the difference between these account types.

### Local and Domain User Accounts

Windows 7 supports two kinds of users: local users and domain users. A computer that is running Windows 7 has the ability to store its own user accounts database. The users stored at the local computer are known as local user accounts.

Active Directory is a directory service that is available with the Windows Server 2008, Windows Server 2003, and Windows 2000 Server platforms. It stores information in a central database called Active Directory that allows users to have a single user account for the network. The users stored in Active Directory's central database are called domain user accounts.

If you use local user accounts, they must be configured on each computer that the user needs access to within the network. For this reason, domain user accounts are commonly used to manage users on any network with more than 10 users.

On Windows 7, Windows Server 2008, Windows Server 2003, Windows XP, and Windows 7 computers you can create local users through the Local Users and Groups utility, as described in the section ''Working with User Accounts,'' later in this chapter. On Windows Server 2008, Windows Server 2003, and Windows 2000 Server domain controllers, you manage users with the Microsoft Active Directory Users and Computers utility.

#### Windows Server 2008

Active Directory is covered in more detail in Chapter 12, ''Networking with Windows Server 2008.'' But if you are looking for a book that covers Active Directory in detail, refer to *MCTS: Windows Server 2008 Active Directory Configuration Study Guide*, by William Panek and James Chellis (Sybex, 2008).

Now that we've looked at the different types of users, let's see how to use accounts to log on and log off the local machine or domain.

## Logging On and Logging Off

Users and administrators must log on to a Windows 7 computer before they can use that computer. When you create user accounts, you set up the computer to accept the logon information provided by the Windows 7 user. You can log on locally to a Windows 7 computer using a local computer account, or you can log on to a domain using an Active Directory account.

When you install the computer, you specify that it will be a part of a workgroup, which implies a local logon, or that the computer will be a part of a domain, which implies a domain logon.

When users are ready to stop working on a Windows 7 computer, they should log off. Users can log off using the Windows Security dialog box.

In the following sections, you will learn about local user authentication and how a user logs out of a Windows 7 computer.

### Local User Logon Authentication Process

Depending on whether you are logging on to a computer locally or are logging into a domain, Windows 7 uses two different logon procedures. When you log on to a Windows 7 computer locally, you must present a valid username and password (ones that exist within the local accounts database). As part of a successful authentication, the following steps take place:

1. At system startup, the user is prompted to click their username from a list of users who have been created locally. This is significantly different from the Ctrl+Alt+Del logon sequence that was used by earlier versions of Windows. The Ctrl+Alt+Del sequence is still used when you log on to a domain environment. You can also configure the Ctrl+Alt+Del logon sequence as an option in a local environment.
2. The local computer compares the user's logon credentials with the information in the local security database.
3. If the information presented matches the account database, an access token is created. Access tokens are used to identify the user and the groups of which that user is a member.

### Access Tokens

Access tokens are created only when you log on. If you change group memberships, you need to log off and log on again to update the access token.

Other actions that take place as part of the logon process include the following list:

- The system reads the part of the Registry that contains user configuration information.
- The user's profile is loaded. (User profiles are discussed in the section ''Setting Up User Profiles, Logon Scripts, and Home Folders,'' later in this chapter.)
- Any policies that have been assigned to the user through a user or Group Policy are enforced. (Policies for users are discussed later in Chapter 9, ''Managing Security.'')
- Any logon scripts that have been assigned are executed. (We discuss assigning logon scripts to users in the ''Setting Up User Profiles, Logon Scripts, and Home Folders'' section.)
- Persistent network and printer connections are restored.

### Permissions

Through the logon process, you can control what resources a user can access by assigning permissions. Permissions are granted to either users or groups. Permissions also determine what actions a user can perform on a computer. In Chapter 9, ''Managing Security,'' you will learn more about assigning resource permissions.

Now that we've seen how a local logon process works, let's explore logging off a Windows 7 machine.

### Logging Off Windows 7

To log off Windows 7, click Start, point to the arrow next to the Shutdown button, and then click Logoff. Pressing Ctrl+Alt+Del also presents you with a screen that allows you to select whether to lock the computer, switch user, log off, change the password, or start Task Manager.

**Real World Scenario**

**Logging Off Computers**

As network administrator, we made it a practice to teach our users to log off their computers every night. What happens in many companies is that users come in on Monday, turn on their computers, and then leave them on and logged in until Friday night.

Having computers logged on to a local machine or to a network all week long is a dangerous practice. This makes it easy for any other user in the company to sit down at their machine and cause trouble. Have your users get into the practice of logging off at night and locking their keyboard when stepping away for break or lunch.

At this point, you should have a good grasp of the various types of accounts on a Windows 7 computer. Next let’s see how to manage these accounts.

## Working with User Accounts

To set up and manage your local user accounts, use the Local Users and Groups utility or the User Accounts utility in Control Panel. With either option, you can create, disable, delete, and rename user accounts, as well as change user passwords.

### Utilizing the Local Users and Groups Utility

Here are the two common methods for accessing the Local Users and Groups utility:

- You can load Local Users and Groups as a Microsoft Management Console (MMC) snap-in. (See Chapter 4, ‘‘Configuring Disks,’’ for details on the MMC and the purpose of snap-ins.)
- You can access the Local Users and Groups utility through the Computer Management utility.

Perform the following steps for accessing the Local Users and Groups utility. The steps first add the Local Users and Groups snap-in MMC to the desktop.

1. Select Start. In the search box, type **MMC**, and then press Enter.
2. If a warning box appears, click Yes.
3. Select File ➢ Add/Remove Snap-in.
4. Scroll down the list, highlight Local Users and Groups, and then click the Add button, as shown in Figure 8.3.
5. In the Choose Target Machine dialog box, click the Finish button to accept the default selection of Local Computer.

6. Click OK in the Add Or Remove Snap-in dialog box.

7. In the MMC window, right-click the Local Users and Groups folder and choose New Window From Here. You will see that Local Users and Groups is now the main window.

8. Click File ➤ Save As. Name the console **Local Users and Groups** and make sure you save it to the Desktop using the Save In drop-down box, as shown in Figure 8.4. Click the Save button.

9. Close the MMC Snap-in.

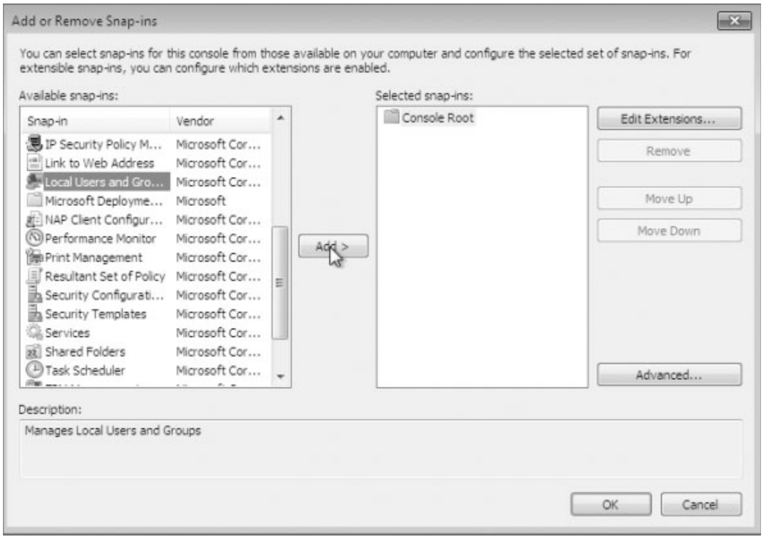


**FIGURE 8.3**
Local Users and Groups snap-in

Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

| Snap-in | Vendor |
|---|---|
| IP Security Policy M... | Microsoft Cor... |
| Link to Web Address | Microsoft Cor... |
| Local Users and Gro... | Microsoft Cor... |
| Microsoft Deployme... | Microsoft |
| NAP Client Configur... | Microsoft Cor... |
| Performance Monitor | Microsoft Cor... |
| Print Management | Microsoft Cor... |
| Resultant Set of Policy | Microsoft Cor... |
| Security Configurati... | Microsoft Cor... |
| Security Templates | Microsoft Cor... |
| Services | Microsoft Cor... |
| Shared Folders | Microsoft Cor... |
| Task Scheduler | Microsoft Cor... |

Selected snap-ins:

Console Root

Description:

Manages Local Users and Groups

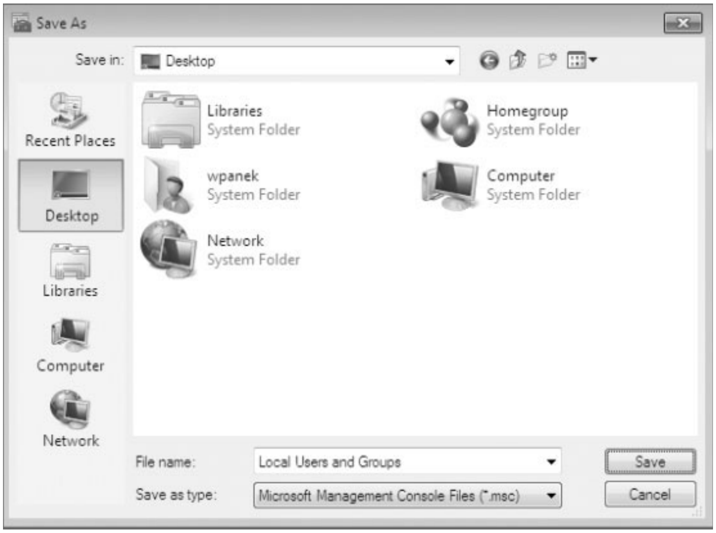


**FIGURE 8.4**
Saving the Local Users and Groups console

Save As

Save in: Desktop

File name: Local Users and Groups

Save as type: Microsoft Management Console Files (*.msc)

You should now see the Local Users and Groups snap-in on your Desktop. You can also open the Local Users and Groups MMC from the Computer Management utility.

Perform the following steps for opening the Local Users and Groups utility from the Computer Management utility:

1. Select Start and then right-click My Computer and select Manage.
2. In the Computer Management window, expand the System Tools folder and then the Local Users and Groups folder.

**COMPUTER MANAGEMENT UTILITY**

If your computer doesn't have the MMC configured, the quickest way to access the Local Users and Groups utility is through the Computer Management utility.

Now let's look at another way to configure users and groups: using the User Accounts utility in Control Panel.

## Using the User Accounts Utility in Control Panel

The User Accounts utility in Control Panel provides the ability to manage user accounts, in addition to configuring parental controls. To access this utility, click Start ➤ Control Panel ➤ User Accounts. Table 8.1 shows the configurable options in User Accounts.

After you install Windows 7, you must create user accounts for users who will be accessing the machine. Let's take a look at this process.

## Creating New Users

To create users on a Windows 7 computer, you must be logged on as a user with permissions to create a new user, or you must be a member of the Administrators group. In the following sections, you will learn about username rules and conventions, usernames, and security identifiers in more detail.

### USERNAME RULES AND CONVENTIONS

The only requirement for creating a new user is that you must provide a valid username. ''Valid'' means that the name must follow the Windows 7 rules for usernames. However, it's also a good idea to have your own rules for usernames, which form your naming convention.

The following rules apply to Windows 7 usernames:

- A username must be from 1 to 20 characters.
- The username must be unique to all other user and group names stored on that specified computer.
- The username cannot contain the following characters:

  * / \ [ ] : ; | = , + ? < > '' @
- A username cannot consist exclusively of periods or spaces.

**TABLE 8.1:** Configurable User Account Options

| OPTION | EXPLANATION |
|---|---|
| Change Your Password | This allows a user to change their password. |
| Remove Your Password | Allows you to remove a password from a user's account. |
| Change Your Picture | Allows you to change the account picture. |
| Change Your Account Name | Allows you to rename the account. |
| Change Your Account Type | Allows you to change your account type from Standard User to Administrator, or vice versa. |
| Manage Another Account | Allows you to configure other accounts on the Windows 7 machine. |
| Change UUAC Settings | Allows you to set the level of notification when changes are made to a user's computer. These notifications can prevent potentially hazardous programs from being loaded onto the operating system. |
| Manage Your Credentials | Allows you to set up credentials that easily enable you to connect to websites that require usernames and passwords or computers that require certificates. |
| Create A Password Reset Disk | Allows you to create a disk that users can use when they forget their password. |
| Link Online IDs | Allows you to link an Online ID with your Windows account. This makes it easier to share files with other computers. |
| Manage Your File Encryption Certificates | Allows you to manage your file encryption certificates. |
| Configure Advanced User Profile Properties | This link brings you directly to the User's Profile dialog box in Control Panel ➢ System ➢ Advanced ➢ System Settings. |
| Change My Environment Variables | Allows you to access the Environment Variables dialog box directly. |

Keeping these rules in mind, you should choose a naming convention (a consistent naming format). For example, consider a user named William Panek. One naming convention might use the last name and first initial, for the username WillP or WilliamP. Another naming convention might use the first initial and last name, for the username WPanek.

Other user-naming conventions are based on the naming convention defined for email names, so that the logon name and email name match. You should also provide a mechanism that would accommodate duplicate names. For example, if you had a user named Jane Smith and a user named John Smith, you might use a middle initial for usernames, such as JDSmith and JRSmith.

It is also a good practice to come up with a naming convention for groups, printers, and computers.

### Naming Conventions

It's not a good practice to use the first name, first letter of the user's last name, as in WilliamP. In a mid-sized to large company, there are greater chances of having two WilliamP users' accounts, but the odds that you will have two WPaneks are rare.

If you choose to use the first name, first letter of the last name option, it can be a lot of work to go back and change this format later if the company grows larger. Choose a naming convention that can grow with the company.

Now let's look at how usernames get a special ID number associated with the account and how that number affects your accounts.

## Usernames and Security Identifiers

When you create a new user, a security identifier (SID) is automatically created on the computer for the user account. The username is a property of the SID. For example, a user SID might look like this:

```
S-1-5-21-823518204-746137067-120266-629-500
```

It's apparent that using SIDs for user identification would make administration a nightmare. Fortunately, for your administrative tasks, you see and use the username instead of the SID.

SIDs have several advantages. Because Windows 7 uses the SID as the user object, you can easily rename a user while still retaining all the properties of that user. The reason is that all security settings get associated with the SID and not the user account.

SIDs also ensure that if you delete and re-create a user account with the same username, the new user account will not have any of the properties of the old account because it is based on a new, unique SID. Every time you create a new user, a unique SID gets associated. Even if the username is the same as a previously deleted account, the system still sees the username as a new user.

Because every user account gets a unique SID number, it is a good practice to disable accounts for users who leave the company instead of deleting the accounts. If you ever need to access the disabled account again, you can do so. Disabling user accounts and deleting user accounts are discussed in detail in the next two sections.

When you create a new user, there are many options that you have to configure for that user. Table 8.2 describes all the options available in the New User dialog box.

**Table 8.2:** User Account Options Available in the New User Dialog Box

| Option | Description |
|---|---|
| User Name | Defines the username for the new account. Choose a name that is consistent with your naming convention (for example, WPanek). This is the only required field. Usernames are not case sensitive. |

**TABLE 8.2:** User Account Options Available in the New User Dialog Box (*CONTINUED*)

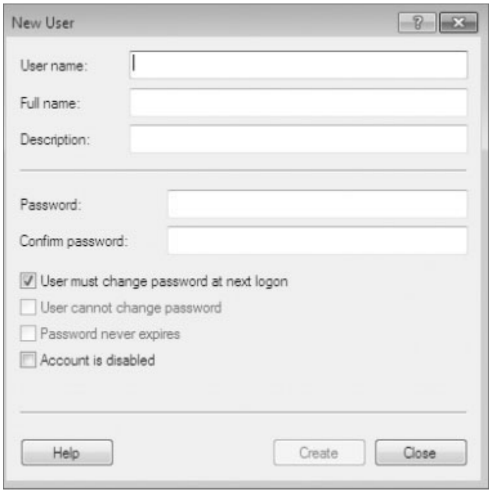
| **OPTION** | **DESCRIPTION** |
|---|---|
| Full Name | Allows you to provide more detailed name information. This is typically the user's first and last names (for example, Will Panek). By default, this field contains the same name as the User Name field. |
| Description | Typically used to specify a title and/or location (for example, Sales-Nashville) for the account, but it can be used to provide any additional information about the user. |
| Password | Assigns the initial password for the user. For security purposes, avoid using readily available information about the user. Passwords are case sensitive. |
| Confirm Password | Confirms that you typed the password the same way two times to verify that you entered the password correctly. |
| User Must Change Password at Next Logon | If enabled, forces the user to change the password the first time they log on. This is done to increase security. By default, this option is selected. |
| User Cannot Change Password | If enabled, prevents a user from changing their password. It is useful for accounts such as Guest and accounts that are shared by more than one user. By default, this option is not selected. |
| Password Never Expires | If enabled, specifies that the password will never expire, even if a password policy has been specified. For example, you might enable this option if this is a service account and you do not want the administrative overhead of managing password changes. By default, this option is not selected. |
| Account Is Disabled | If enabled, specifies that this account cannot be used for logon purposes. For example, you might select this option for template accounts or if an account is not currently being used. It helps keep inactive accounts from posing security threats. By default, this option is not selected. |

Perform the following steps to create a new local user account. Before you complete these steps, make sure you are logged on as a user with permissions to create new users and have already added the Local Users and Groups snap-in to the MMC.

1. Open the Admin Console MMC desktop shortcut that was created in the previous steps and expand the Local Users and Groups snap-in. If a dialog box appears, click Yes.
2. Highlight the Users folder and select Action ➢ New User. The New User dialog box appears, as shown in Figure 8.5.
3. In the User Name text box, type **CPanek**.
4. In the Full Name text box, type **Crystal Panek**.
5. In the Description text box, type **Operations Manager**.

6. Leave the Password and Confirm Password text boxes empty and accept the defaults for the check boxes. Make sure you deselect the User Must Change Password At Next Logon option. Click the Create button to add the user.

**Figure 8.5**
New User dialog box



☑ User must change password at next logon
□ User cannot change password
□ Password never expires
□ Account is disabled

7. Use the New User dialog box to create six more users, filling out the fields as follows:

   - Name: **WPanek**; Full Name: **Will Panek**; Description**: IT Admin**; Password: (blank)
   - Name: **TWentworth**; Full Name: **Tylor Wentworth**; Description: **Cisco Admin**; Password: (blank)
   - Name: **GWashington**; Full Name: **George Washington**; Description: **President**; Password: **P@ssw0rD**
   - Name: **JAdams**; Full Name: **John Adams**; Description: **Vice President**; Password: **v!$t@**
   - Name: **BFranklin**; Full Name: *Ben Franklin*; Description: **NH Sales Manager**; Password: **P3@ch** (with a capital P)
   - Name: **ALincoln**; Full Name: **Abe Lincoln**; Description: **Tech Support**; Password: **Bearded1** (capital B)

8. After you finish creating all the users, click the Close button to exit the New User dialog box.

> **Command-Line Utility**
>
> You can also create users through the command-line utility NET USER. For more information about this command, type **NET USER /?** at a command prompt.

As we stated earlier, it's a good practice to disable accounts for users who leave the company. Let's look at that process.

## Disabling User Accounts

When a user account is no longer needed, the account should be disabled or deleted. After you've disabled an account, you can later enable it again to restore it with all of its associated user properties. An account that is deleted, however, can never be recovered.

### Security Threats

User accounts not in use pose a security threat because an intruder could access your network through an inactive account. User accounts that are no longer needed should be disabled immediately.

You might disable an account because a user will not be using it for a period of time, perhaps because that employee is going on vacation or taking a leave of absence. Another reason to disable an account is that you're planning to put another user in that same function.

For example, suppose that Gary, the engineering manager, quits. If you disable his account, when your company hires a new engineering manager, you can simply rename Gary's user account (to the username for the new manager) and enable that account. This ensures that the user who takes over Gary's position will have all the same user properties and own all the same resources.

Disabling accounts also provides a security mechanism for special situations. For example, if your company were laying off a group of people, a security measure would be to disable their accounts at the same time the layoff notices were given out. This prevents those users from inflicting any damage to the company's files after they receive their layoff notice.

Perform the following steps to disable a user account. Before you complete these steps, you should have already created new users, as shown in the previous section.

1. Open the Admin Console MMC desktop shortcut and expand the Local Users and Groups snap-in.
2. Open the Users folder. Double-click user WPanek to open his Properties dialog box.
3. In the General tab, check the Account Is Disabled box. Click OK.
4. Close the Local Users and Groups MMC.
5. Log off and attempt to log on as WPanek. This should fail because the account is now disabled.
6. Log back on using your user account.

### Properties Shortcut

Another option for accessing a user's properties is to highlight the user, right-click, and select Properties.

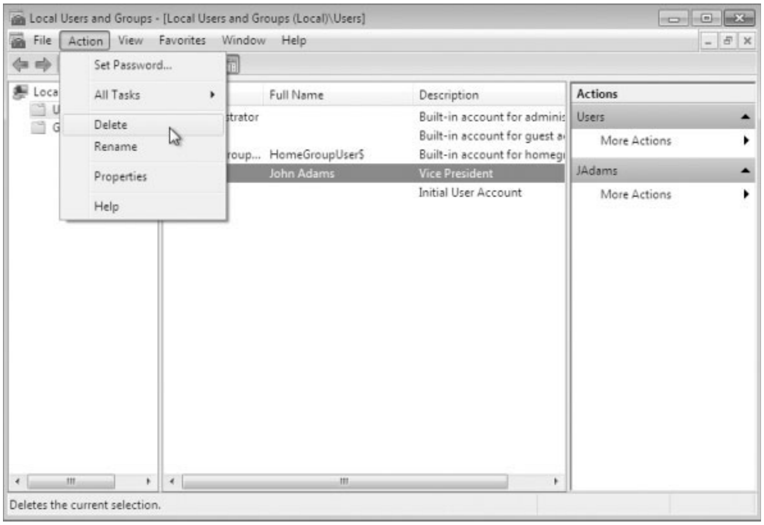
Now when users have left a company for a long period of time and you know you no longer need the user account, you can delete the account. Let's look at how to delete user accounts.

## Deleting User Accounts

As noted in the preceding section, you should disable a user account if you are not sure that the account will ever be needed again. But if the account has been disabled and you know that the user account will never need access again, you should then delete the account.

To delete a user, open the Local Users and Groups utility, highlight the user account you want to delete, and click Action to bring up the menu, as shown in Figure 8.6. Then select Delete. You can also delete an account by clicking the account and pressing the Delete key on the keyboard.

**FIGURE 8.6**
Deleting a user account

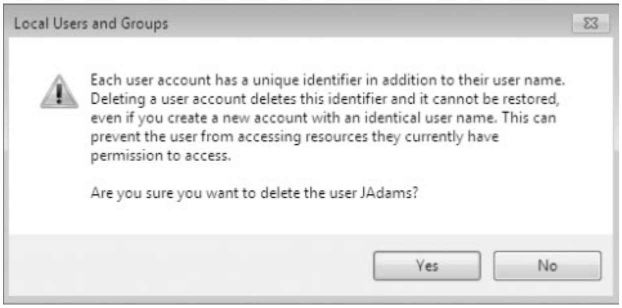


| | Full Name | Description |
|---|---|---|
| trator | | Built-in account for adminis |
| | | Built-in account for guest a |
| roup... | HomeGroupUser$ | Built-in account for homegı |
| | John Adams | Vice President |
| | | Initial User Account |

Deletes the current selection.

Because user deletion is a permanent action, you see the dialog box shown in Figure 8.7 that asks you to confirm that you really want to delete the account. After you click the Yes button, you will not be able to re-create or reaccess the account (unless you restore your local user accounts database from a backup).

**FIGURE 8.7**
Confirming user deletion



Each user account has a unique identifier in addition to their user name. Deleting a user account deletes this identifier and it cannot be restored, even if you create a new account with an identical user name. This can prevent the user from accessing resources they currently have permission to access.

Are you sure you want to delete the user JAdams?

Perform the following steps to delete a user account. These steps assume you have completed the previous steps in this chapter.

1. Open the Admin Console MMC Desktop shortcut and expand the Local Users and Groups snap-in.
2. Expand the Users folder and single-click on user JAdams to select his user account.
3. Select Action ➤ Delete. The dialog box for confirming user deletion appears.
4. Click Yes to confirm that you want to delete this user.
5. Close the Local Users and Groups MMC.

Now that we have disabled and deleted accounts, let's see how to rename a user's account.

## Renaming User Accounts

After you have created an account, you can rename the account at any time. Renaming a user account allows the user to retain all the associated user properties of the previous username. As noted previously in the chapter, the name is a property of the SID.

You might want to rename a user account because the user's name has changed (for example, the user got married) or because the name was spelled incorrectly. Also, as explained in the ''Disabling User Accounts'' section, you can rename an existing user's account for a new user, such as someone hired to take an ex-employee's position, when you want the new user to have the same properties.

Perform the following steps to rename a user account. These steps assume you have completed all of the previous steps in this chapter.

1. Open the Admin Console MMC shortcut and expand the Local Users and Groups snap-in.
2. Open the Users folder and highlight user ALincoln.
3. Select Action ➤ Rename.
4. Type the username **RReagan** and press Enter. Notice that the Full Name retained the original property of Abe Lincoln in the Local Users and Groups utility.
5. Double-click RReagan to open their properties and change the user's full name to **Ronald Reagan**.
6. Click the User Must Change Password At Next Logon checkbox.
7. Click OK.
8. Close the Local Users and Groups MMC.

### Renamed User's Properties

Renaming a user does not change any ''hard-coded'' names, such as the user's home folder. If you want to change these names as well, you need to modify them manually, for example, through Windows Explorer.

Another common task that we must deal with is resetting the user's password. You'll learn how next.

### Changing a User's Password

What should you do if a user forgets his password and can't log on? You can't just open a dialog box and see the old password. However, as the administrator, you can change the user's password and then the user can use the new one.

It is important as IT managers and IT administrators to teach your users the proper security measures that go along with password protection. As you have all probably seen before, the users who tape their password to their monitors or under the keyboards need to be taught the correct methods for protecting their passwords.

It's our job as IT professionals to teach our users proper security and it always amazes me when I do consulting how many IT departments don't teach their users properly.

IT personnel should give classes to their users at least once a month on different topics. One of these topics should be proper password security. Teach your users how to protect their passwords and what to do if their passwords get compromised.

Perform the following steps to change a user's password. This exercise assumes you have completed all the previous steps in this chapter.

1. Open the Admin Console MMC Desktop shortcut and expand the Local Users and Groups snap-in.
2. Open the Users folder and highlight user CPanek.
3. Select Action ➢ Set Password. The Set Password dialog box appears.
4. A warning appears that indicates risks are involved in changing the password. Select Proceed.
5. Type the new password and then confirm the password. Click OK.
6. Close the Local Users and Groups MMC.

Now that you have seen how to create users in Windows 7, let's look at configuring and managing your user's properties.

## Managing User Properties

For more control over user accounts, you can configure user properties. Through the user's Properties dialog box, you can change the original password options, add the users to existing groups, and specify user profile information.

To open a user's Properties dialog box, access the Local Users and Groups utility, open the Users folder, and double-click the user account. The user's Properties dialog box has tabs for the three main categories of properties: General, Member Of, and Profile.

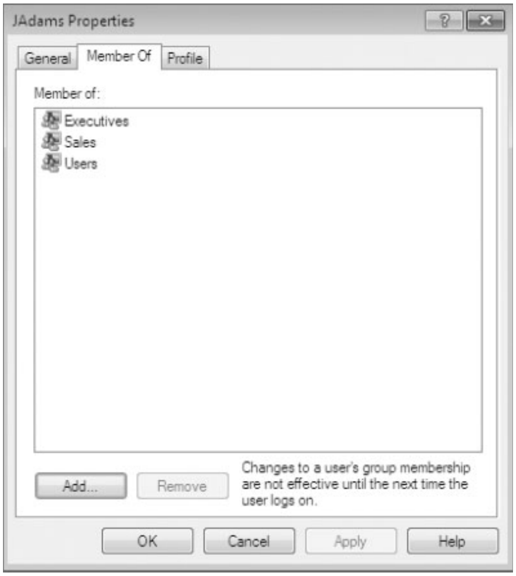
The General tab contains the information you supplied when you set up the new user account, including any Full Name and Description information, the password options you selected, and whether the account is disabled. If you want to modify any of these properties after you've created the user, simply open the user's Properties dialog box and make the changes on the General tab.

You can use the Member Of tab to manage the user's membership in groups. The Profile tab lets you set properties to customize the user's environment. The following sections discuss the Member Of and Profile tabs in detail.

### Managing User Group Membership

The Member Of tab of the user's Properties dialog box displays all the groups that the user belongs to, as shown in Figure 8.8. On this tab, you can add the user to an existing group or remove that user from a group. To add a user to a group, click the Add button and select the group that the user should belong to. If you want to remove the user from a group, highlight the group and click the Remove button.

**FIGURE 8.8**
The Member Of tab of the user's Properties dialog box



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

Perform the following steps to add a user to an existing group. These steps assume you have completed all the previous steps in this chapter.

1. Open the Local Users and Groups MMC Desktop snap-in that you created in the previous steps.
2. Open the Users folder and double-click user WPanek. The WPanek Properties dialog box appears.
3. Select the Member Of tab and click the Add button. The Select Groups dialog box appears.
4. Under Enter The Object Names To Select, type **Backup Operators** and click the Check Names button. After the name is confirmed, click OK.
5. Click OK to close the WPanek Properties dialog box.

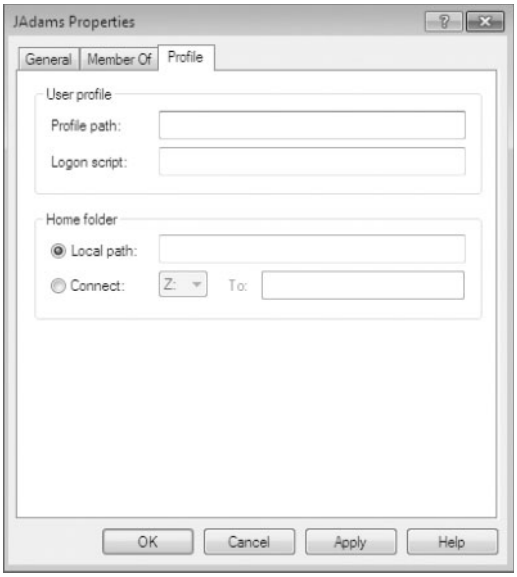
The final tab in the user's properties is called the Profile tab. Now let's look at that Profile tab and the options that you can configure within that tab.

## Setting Up User Profiles, Logon Scripts, and Home Folders

The Profile tab of the user's Properties dialog box, shown in Figure 8.9, allows you to customize the user's environment. Here, you can specify the following items for the user:

- User profile path
- Logon script
- Home folder

**FIGURE 8.9**
The Profile tab of the user's Properties dialog box



The following sections describe how these properties work and when you might want to use them.

## SETTING A PROFILE PATH

User profiles contain information about the Windows 7 environment for a specific user. For example, profile settings include the Desktop arrangement, program groups, and screen colors that users see when they log on.

Each time you log on to a Windows 7 computer, the system checks to see if you have a local user profile in the Users folder, which was created on the boot partition when you installed Windows 7.

### USERS PROFILES

The default location for user profiles is `systemdrive:\Users\UserName`.

If you need to reapply the default user profile for a user, you can delete the user's profile by opening the Control Panel ➢ click System ➢ click Advanced system settings ➢ click Settings in the User Profiles area of the Advanced tab ➢ select the user profile to delete ➢ and click Delete.

The first time users log on, they receive a default user profile. A folder that matches the user's logon name is created for the user in the Users folder. The user profile folder that is created holds a file called `NTUSER.DAT`, as well as subfolders that contain directory links to the user's Desktop items.

Perform the following steps to create two new users and set up local user profiles:

1. Using the Local Users and Groups utility, create two new users: APanek and PPanek. Deselect the User Must Change Password At Next Logon option for each user.
2. Select Start ➢ All Programs ➢ Accessories ➢ Windows Explorer. Expand Computer, then Local Disk (C:), and then Users. Notice that the Users folder does not contain user profile folders for the new users.
3. Log off and log on as APanek.
4. Right-click an open area on the Desktop and select Personalize. In the Personalization dialog box, select a color scheme and click Apply, and then click OK.
5. Right-click an open area on the Desktop and select New ➢ Shortcut. In the Create Shortcut dialog box, type **CALC**. Accept CALC as the name for the shortcut and click Finish.
6. Log off as APanek and log on as PPanek. Notice that user PPanek sees the Desktop configuration stored in the default user profile.
7. Log off as PPanek and log on as APanek. Notice that APanek sees the Desktop configuration you set up in steps 3, 4, and 5.
8. Log off as APanek and log on as your user account. Select Start ➢ All Programs ➢ Accessories ➢ Windows Explorer. Expand Computer, then Local Disk (C:), and then Users. Notice that this folder now contains user profile folders for APanek and PPanek.

The drawback of local user profiles is that they are available only on the computer where they were created. For example, suppose all of your Windows 7 computers are a part of a domain and you use only local user profiles.

User Rick logs on at Computer A and creates a customized user profile. When he logs on to Computer B for the first time, he will receive the default user profile rather than the customized user profile he created on Computer A. For users to access their user profile from any computer they log on to, you need to use roaming profiles; however, these require the use of a network server and they can't be stored on a local Windows 7 computer.

In the next sections, you will learn about how roaming profiles and mandatory profiles can be used. In order to have a roaming profile or a mandatory profile, your computer must be a part of a network with server access.

### *Using Roaming Profiles*

A roaming profile is stored on a network server and allows users to access their user profile, regardless of the client computer to which they're logged on. Roaming profiles provide a consistent Desktop for users who move around, no matter which computer they access. Even if the server that stores the roaming profile is unavailable, the user can still log on using a local profile.

If you are using roaming profiles, the contents of the user's `systemdrive:\Users\UserName` folder will be copied to the local computer each time the roaming profile is accessed. If you have stored large files in any subfolders of your user profile folder, you might notice a significant delay when accessing your profile remotely as opposed to locally.

If this problem occurs, you can reduce the amount of time the roaming profile takes to load by moving the subfolder to another location, such as the user's home directory, or you can use

Group Policy Objects within Active Directory to specify that specific folders should be excluded when the roaming profile is loaded.

### *Using Mandatory Profiles*

A mandatory profile is a profile that can't be modified by the user. Only members of the Administrators group can manage mandatory profiles. You might consider creating mandatory profiles for users who should maintain consistent Desktops.

For example, suppose you have a group of 20 salespeople who know enough about system configuration to make changes but not enough to fix any problems they create. For ease of support, you could use mandatory profiles. This way, all of the salespeople will always have the same profile and will not be able to change their profiles.

You can create mandatory profiles for a single user or a group of users. The mandatory profile is stored in a file named `NTUSER.MAN`. A user with a mandatory profile can set different Desktop preferences while logged on, but those settings will not be saved when the user logs off.

#### Mandatory Profiles

You can use only roaming profiles as mandatory profiles. Mandatory profiles do not work for local user profiles.

There is a second type of mandatory profile called Super Mandatory Profile. Let's look at this other type of profile.

### *Using Super Mandatory Profiles*

A super mandatory profile is a mandatory user profile with an additional layer of security. With mandatory profiles, a temporary profile is created if the mandatory profile is not available when a user logs on. However, when super mandatory profiles are configured, temporary profiles are not created if the mandatory profile is not available over the network, and the user is unable to log on to the computer.

The process for creating super mandatory profiles is similar to creating mandatory profiles, except that instead of renaming the user folder to `Username.v2`, you name the folder `Username.man.v2`.

#### Real World Scenario

#### Copying User Profiles

Within your company you have a user, Paige, who logs in with two different user accounts. One account is a regular user account and the other is an Administrator account used for administrative tasks only.

When Paige established all her Desktop preferences and installed the computer's applications, she used the Administrator account. Now when she logs in with the regular user account, she can't access the Desktop and profile settings that were created for her as an administrative user.

To solve this problem, you can copy a local user profile from one user to another (for example, from Paige's Administrator account to her regular user account). Choose Control Panel ➢ System, click Advanced System Settings, and click the User Profiles Settings button. When you copy a user profile, the following items are copied: Favorites, Cookies, Documents, Start menu items, and other unique user Registry settings.

Another configurable item on the Profile tab of the user's properties is using logon scripts. Let's see how to configure these scripts.

### Configuring Logon Scripts

Logon scripts are files that run every time a user logs on to the network. They are usually batch files, but they can be any type of executable file.

You might use logon scripts to set up drive mappings or to run a specific executable file each time a user logs on to the computer. For example, you could run an inventory management file that collects information about the computer's configuration and sends that data to a central management database. Logon scripts are also useful for compatibility with non–Windows 7 clients who want to log on but still maintain consistent settings with their native operating system.

To run a logon script for a user, enter the script name in the Logon Script text box on the Profile tab of the user's Properties dialog box.

Next we'll look at another item that you can configure on the Profile tab: home folders.

### Setting Up Home Folders

Users usually store their personal files and information in a private folder called a home folder. In the Profile tab of the user's Properties dialog box, you can specify the location of a home folder as a local folder or a network folder.

To specify a local path folder, choose the Local Path option and type the path in the text box next to that option. To specify a network path for a folder, choose the Connect option and specify a network path using a Universal Naming Convention (UNC) path.

A UNC consists of the computer name and the share that has been created on the computer. In this case, a network folder should already be created and shared. For example, if you wanted to connect to a folder called `\Users\Will` on a server called SALES, you'd choose the Connect option, select a drive letter that would be mapped to the home directory, and then type **`\\SALES\Users\Will`** in the To box.

If the home folder you are specifying does not exist, Windows 7 attempts to create the folder for you. You can also use the variable `%username%` in place of a specific user's name.

Perform the following steps to assign a home folder to a user. These steps assume you have completed all the previous steps in this chapter.

1. Open the Admin Console MMC desktop shortcut and expand the Local Users and Groups snap-in.
2. Open the Users folder and double-click user WPanek. The WPanek Properties dialog box appears.
3. Select the Profile tab and click the Local Path radio button to select it.
4. Specify the home folder path by typing **`C:\HomeFolders\WPanek`** in the text box for the Local Path option. Then click OK.

5. Use Windows Explorer to verify that this folder was created.
6. Close the Local Users and Groups MMC.

**Real World Scenario**

**Managing Home Folders**

As an administrator for a large network, one of my primary responsibilities is to make sure that all data is backed up daily. This practice can be difficult because making daily backups of each user's local hard drive is impractical. You can also have problems with employees deleting important corporate information as they are leaving the company.

After examining the contents of a typical user's local drive, you will realize that most of the local disk space is taken by the operating system and the user's stored applications. This information does not change and does not need to be backed up. What we are primarily concerned with is backing up the user's data.

To more effectively manage this data and accommodate the necessary backup, you should create home folders for each user, stored on a network share. This allows the data to be backed up daily, to be readily accessible should a local computer fail, and to be easily retrieved if the user leaves the company.

Here are the steps to create a home folder that resides on the network. Decide which server will store the users' home folders, create a directory structure that will store the home folders efficiently (for example, `C:\HOME`), and create a single share to the home folder. Then use NTFS and share permissions to ensure that only the specified user has permissions to their home folder. Setting permissions is covered in Chapter 9, ''Managing Security.'' After you create the share and assign permissions, you can specify the location of the home folder on the Profile tab of the user's Properties dialog box.

After you create your users' accounts, there is a possibility that you can run into errors or issues with the user's accounts. In the next section we look at how to troubleshoot user account issues.

# Troubleshooting User Accounts Authentication

When a user attempts to log on through Windows 7 and is unable to be authenticated, you need to track down the reason for the problem.

The following sections offer some suggestions that can help you troubleshoot logon authentication errors for local and domain user accounts.

## Troubleshooting Local User Account Authentication

If a local user is having trouble logging on, the problem might be with the username, with the password, or the user account itself. The following list gives some common causes of local logon errors:

**Incorrect Username** You can verify that the username is correct by checking the Local Users and Groups utility. Verify that the name was spelled correctly.

**Incorrect Password** Remember that passwords are case sensitive. Is the Caps Lock key on? If you see any messages that relate to an expired password or locked-out account, the reason for the problem is obvious. If necessary, you can assign a new password through the Local Users and Groups utility.

**Prohibitive User Rights** Does the user have permission to log on locally at the computer? By default, the Log On Locally user right is granted to the Users group, so all users can log on to Windows 7 computers.

However, if this user's right was modified, you will see an error message stating that the local policy of this computer does not allow interactive logon. The terms *interactive logon* and *local logon* are synonymous and mean that the user is logging on at the computer where the user account is stored on the computer's local database.

**A Disabled or Deleted Account** You can verify whether an account has been disabled or deleted by checking the account properties using the Local Users and Groups utility.

**A Domain Account Logon at the Local Computer** If a computer is part of a domain, the logon dialog box has options for logging on to the domain or to the local computer. Make sure that the user has chosen the correct option.

You might also have issues with logging onto the domain. In the next section we look at how to troubleshoot domain accounts.

## Troubleshooting Domain User Accounts Authentication

Troubleshooting a logon problem for a user with a domain account involves checking the same areas as you do for local account logon problems, as well as a few others.

We cover domain accounts in detail in Chapter 12, but let's cover some of the issues you might encounter with domain accounts authentication.

The following list gives some common causes of domain logon errors:

**Incorrect Password** As with local accounts, check that the password was entered in the proper case (and the Caps Lock key isn't on), the password hasn't expired, and the account has not been locked out. If the password still doesn't work, you can assign a new password using the Active Directory Users and Computers utility.

**Incorrect Username** You can verify that the username is correct by checking the Active Directory Users and Computers utility to verify that the name was spelled correctly.

**Prohibitive User Rights** Does the user have permission to log on locally at the computer? This assumes that the user is attempting to log on to the domain controller. Regular users do not have permission to log on locally at the domain controller. The assumption is that users will log on to the domain from network workstations. If the user has a legitimate reason to log on locally at the domain controller, that user should be assigned the Log On Locally user right.

**A Disabled or Deleted Account** You can verify whether an account has been disabled or deleted by checking the account properties using the Active Directory Users and Computers utility.

**A Local Account Logon at a Domain Computer** Is the user trying to log on with a local user account name instead of a domain account? Make sure that the user has selected to log on to a domain in the Logon dialog box.

**The Computer Being Used Is Not Part of the Domain** Is the user sitting at a computer that is part of the domain to which the user is trying to log on? If the Windows 7 computer is not part of the domain that contains the user account or does not have a trust relationship defined with the domain that contains the user account, the user will be unable to log on.

**Unavailable Domain Controller, DNS Server, or Global Catalog** Is the domain controller available to authenticate the user's request? If the domain controller is down for some reason, the user will be unable to log on until it comes back up (unless the user logs on using a local user account). A DNS server and the Global Catalog for Active Directory are also required.

When a user login is successful, the logon credentials are saved to local cache. The next time the user attempts to log on, the cached credentials can be used to log on in the event that they can't be authenticated by a domain controller.

If Group Policies have been updated and a user is using cached credentials, the new Group Policy updates will not be applied. If you want to force a user to log on using noncached credentials, you can set the number of cached credentials to 0 using a Group Policy. Group Policy is covered in detail in Chapter 9.

After creating user accounts, normally we place these user accounts into groups, which we discuss in the next section.

## Creating and Managing Groups

Groups are an important part of network management. Many administrators are able to accomplish the majority of their management tasks through the use of groups; they rarely assign permissions to individual users.

Windows 7 includes built-in local groups, such as Administrators and Backup Operators. These groups already have all the permissions needed to accomplish specific tasks. Windows 7 also uses default special groups, which are managed by the system. Users become members of special groups based on their requirements for computer and network access.

You can create and manage local groups through the Local Users and Groups utility. With this utility, you can add groups, change group membership, rename groups, and delete groups.

One misconception with groups is that they have to work with Group Policy Objects (GPOs). This is not correct. GPOs are a set of rules that allow you to set computer configuration and user configuration options that apply to users or computers. Group Policies are typically used with Active Directory and are applied as GPOs. GPOs are discussed in detail in Chapter 9, ''Managing Security.''

In the following sections, you will learn about groups and all the built-in groups. Then you will learn how to create and manage these groups.

### Using Built-in Groups

On a Windows 7 computer, default local groups have already been created and assigned all necessary permissions to accomplish basic tasks. In addition, there are built-in special groups that the Windows 7 system handles automatically. These groups are described in the following sections.

**Using Default Local Groups** A local group is a group that is stored on the local computer's accounts database. These are the groups you can add users to and can manage directly on a Windows 7 computer. By default, the following local groups are created on Windows 7 computers:

- Administrators
- Backup Operators
- Cryptographic Operators
- Distributed COM Users
- Event Log Readers
- Guests
- IIS_IUSRS
- Network Configuration Operators
- Performance Log Users
- Performance Monitor Users
- Power Users
- Remote Desktop Users
- Replicator
- Users

We briefly describe each group, its default permissions, and the users assigned to the group by default.

### Built-in Groups

If possible, you should add users to the built-in local groups rather than creating new groups from scratch. This simplifies administration because the built-in groups already have the appropriate permissions. All you need to do is add the users whom you want to be members of the group.

**The Administrators Group** The Administrators group has full permissions and privileges. Its members can grant themselves any permissions they do not have by default to manage all the objects on the computer. (Objects include the file system, printers, and account management.) By default, the Administrator account, which is disabled by default, and the initial user account are members of the Administrators local group.

### Administrators Group

Assign users to the Administrators group with caution because they will have full permissions to manage the computer.

Members of the Administrators group can perform the following tasks:

- Install the operating system.
- Install and configure hardware device drivers.
- Install system services.
- Install service packs, hot fixes, and Windows updates.
- Upgrade the operating system.
- Repair the operating system.
- Install applications that modify the Windows system files.
- Configure password policies.
- Configure audit policies.
- Manage security logs.
- Create administrative shares.
- Create administrative accounts.
- Modify groups and accounts that have been created by other users.
- Remotely access the Registry.
- Stop or start any service.
- Configure services.
- Increase and manage disk quotas.
- Increase and manage execution priorities.
- Remotely shut down the system.
- Assign and manage user rights.
- Reenable locked-out and disabled accounts.
- Manage disk properties, including formatting hard drives.
- Modify systemwide environment variables.
- Access any data on the computer.
- Back up and restore all data.

**The Backup Operators Group** Members of the Backup Operators group have permissions to back up and restore the file system, even if the file system is NTFS and they have not been assigned permissions to access the file system. However, the members of Backup Operators can access the file system only using the Backup utility. To access the file system directly, Backup Operators must have explicit permissions assigned. There are no default members of the Backup Operators local group.

**The Cryptographic Operators Group** The Cryptographic Operators group has access to perform cryptographic operations on the computer. There are no default members of the Cryptographic Operators local group.

**The Distributed COM Users Group** The Distributed COM Users group has the ability to launch and run Distributed COM objects on the computer. There are no default members of the Distributed COM Users local group.

**The Event Log Readers Group** The Event Log Readers group has access to read the event log on the local computer. There are no default members of the Event Log Readers local group.

**The Guests Group** The Guests group has limited access to the computer. This group is provided so that you can allow people who are not regular users to access specific network resources. As a general rule, most administrators do not allow Guest access because it poses a potential security risk. By default, the Guest user account is a member of the Guests local group.

**The IIS_IUSRS Group** The IIS_IUSRS group is used by Internet Information Services (IIS). The NT AUTHORITY\IUSR user account is a member of the IIS_IUSRS group by default.

**The Network Configuration Operators Group** Members of the Network Configuration Operators group have some administrative rights to manage the computer's network configuration — for example, editing the computer's TCP/IP settings.

**The Performance Log Users Group** The Performance Log Users group has the ability to access and schedule logging of performance counters and can create and manage trace counters on the computer.

**The Performance Monitor Users Group** The Performance Monitor Users group has the ability to access and view performance counter information on the computer. Users who are members of this group can access performance counters both locally and remotely.

**The Power Users Group** The Power Users group is included in Windows 7 for backward compatibility. The Power Users group is included to ensure that computers upgraded from Windows XP function as before with regard to folders that allow access to members of the Power Users group. Otherwise, the Power Users group has limited administrative rights.

**The Remote Desktop Users Group** The Remote Desktop Users group allows members of the group to log on remotely for the purpose of using the Remote Desktop service.

**The Replicator Group** The Replicator group is intended to support directory replication, which is a feature that domain servers use. Only domain users who will start the replication service should be assigned to this group. The Replicator local group has no default members.

**The Users Group** The Users group is intended for end users who should have very limited system access. If you have installed a fresh copy of Windows 7, the default settings for the Users group prohibit its members from compromising the operating system or program files. By default, all users who have been created on the computer, except Guest, are members of the Users local group.

Another type of group that is used by Windows 7 is special groups. In the next section we will look at special groups and how they work.

## Using Special Groups

Special groups can be used by the system or by administrators. Membership in these groups is automatic if certain criteria are met. You cannot manage special groups through the Local Users and Groups utility, but an administrator can add these special groups to resources. Table 8.3 describes several of the special groups that are built into Windows 7.

**TABLE 8.3:** Special Groups in Windows 7

| GROUP | DESCRIPTION |
|---|---|
| Anonymous Logon | This group includes users who access the computer through anonymous logons. When users gain access through special accounts created for anonymous access to Windows 7 services, they become members of the Anonymous Logon group. |
| Authenticated Users | This group includes users who access the Windows 7 operating system through a valid username and password. Users who can log on belong to the Authenticated Users group. |
| Batch | This group includes users who log on as a user account that is used only to run a batch job. Batch job accounts are members of the Batch group. |
| Creator Owner | This is the account that created or took ownership of the object and is typically a user account. Each object (files, folders, printers, and print jobs) has an owner. Members of the Creator Owner group have special permissions to resources. For example, if you are a regular user who has submitted 12 print jobs to a printer, you can manipulate your print jobs as Creator Owner, but you can't manage any print jobs submitted by other users. |
| Dialup | This group includes users who log on to the network from a dial-up connection. Dial-up users are members of the Dialup group. |
| Everyone | This group includes anyone who could possibly access the computer. The Everyone group includes all users who have been defined on the computer (including Guest), plus (if your computer is a part of a domain) all users within the domain. If the domain has trust relationships with other domains, all users in the trusted domains are part of the Everyone group as well. The exception to automatic group membership with the Everyone group is that members of the Anonymous Logon group are not included as a part of the Everyone group. |
| Interactive | This group includes all users who use the computer's resources locally. Local users belong to the Interactive group. |
| Network | This group includes users who access the computer's resources over a network connection. Network users belong to the Network group. |
| Service | This group includes users who log on as a user account that is used only to run a service. You can configure the use of user accounts for logon through the Services program, and these accounts become members of the Service group. |
| System | When the system accesses specific functions as a user, that process becomes a member of the System group. |
| Terminal Server User | This group includes users who log on through Terminal Services. These users become members of the Terminal Server User group. |

Now that we have looked at the different types of groups, let's explore at how to manage and work with these groups.

## Working with Groups

Groups are used to logically organize users with similar rights requirements. Groups simplify administration because you can manage a few groups rather than many user accounts. For the same reason, groups simplify troubleshooting. Users can belong to as many groups as needed, so it's not difficult to put users into groups that make sense for your organization.

For example, suppose Jane is hired as a data analyst to join the four other data analysts who work for your company. You sit down with Jane and create an account for her, assigning her the network permissions for the access you think she needs. Later, however, you find that the four other data analysts (who have similar job functions) sometimes have network access Jane doesn't have, and sometimes she has access they don't have. This is happening because all their permissions were assigned individually and months apart.

To avoid such problems and reduce your administrative workload, you can assign all the company's data analysts to a group and then assign the appropriate permissions to that group. Then, as data analysts join or leave the department, you can simply add them to or remove them from the group.

You can create new groups for your users, and you can use the Windows 7 default local built-in groups that were described in the previous section. In both cases, your planning should include checking to see if an existing local group meets your requirements before you decide to create a new group.

For example, if all the users need to access a particular application, it makes sense to use the default Users group rather than creating a new group and adding all the users to that group.

To work with groups, you can use the Local Users and Groups utility. Let's see how to create new groups.

### Creating New Groups

To create a group, you must be logged on as a member of the Administrators group. The Administrators group has full permissions to manage users and groups.

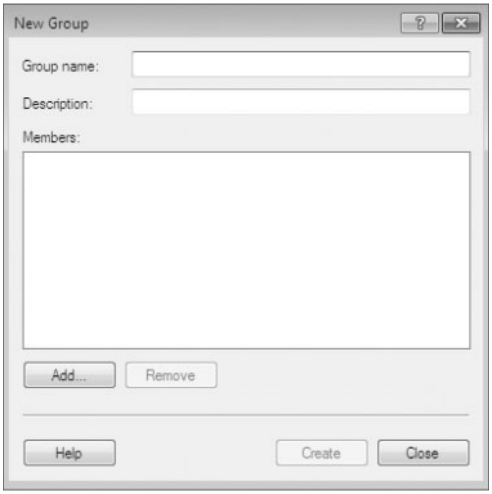
As you do in your choices for usernames, keep your naming conventions in mind when assigning names to groups. When you create a local group, consider the following guidelines:

- The group name should be descriptive (for example, Accounting Data Users).
- The group name must be unique to the computer, different from all other group names and usernames that exist on that computer.
- Group names can be up to 256 characters. It is best to use alphanumeric characters for ease of administration. Most special characters — for example, backslash (\) — are not allowed.

Creating groups is similar to creating users, and it is a fairly easy process. After you've added the Local Users and Groups MMC or use the Local Users and Groups through Computer Management, expand it to see the Users and Groups folders. Right-click the Groups folder and select New Group from the context menu. This brings up the New Group dialog box, as shown in Figure 8.10.

The only required entry in the New Group dialog box is the group name. If appropriate, you can enter a description for the group, and you can add (or remove) group members. When you're ready to create the new group, click the Create button.

**FIGURE 8.10**
The New Group dialog box



Perform the following steps to create two new local groups:

1. Open the Admin Console MMC Desktop shortcut you created and expand the Local Users and Groups snap-in.
2. Right-click the Groups folder and select New Group.
3. In the New Group dialog box, type **Data Users** in the Group Name text box. Click the Create button.
4. In the New Group dialog box, type **Application Users** in the Group Name text box. Click the Create button.

After the groups are created, you have to manage the groups and its membership. In the next section we look at managing groups.

### Managing Group Membership

After you've created a group, you can add members to it. As mentioned earlier, you can put the same user in multiple groups. You can easily add and remove users through a group's Properties dialog box, as shown in Figure 8.11. To access this dialog box from the Groups folder in the Local Users and Groups utility, double-click the group you want to manage.

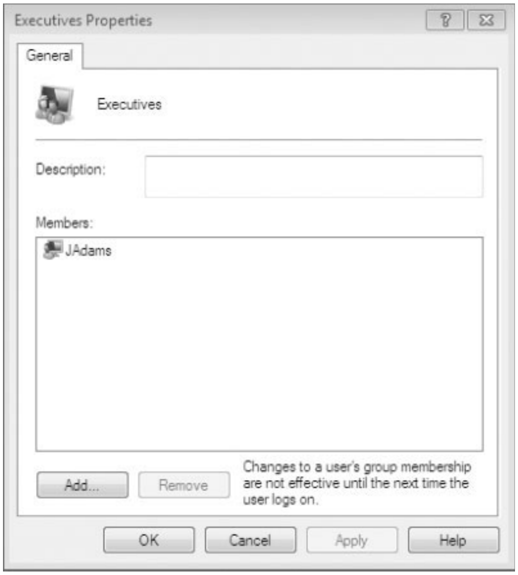
From the group's Properties dialog box, you can change the group's description and add or remove group members. When you click the Add button to add members, the Select Users dialog box appears, as shown in Figure 8.12.

In the Select Users dialog box, enter the object names of the users you want to add. You can use the Check Names button to validate the users against the database. Select the user accounts you want to add and click Add. Click OK to add the selected users to the group.

#### Special Groups

Although the special groups that were covered earlier in the chapter are listed in this dialog box, you cannot manage the membership of these special groups.

**FIGURE 8.11**
A group's Properties dialog box



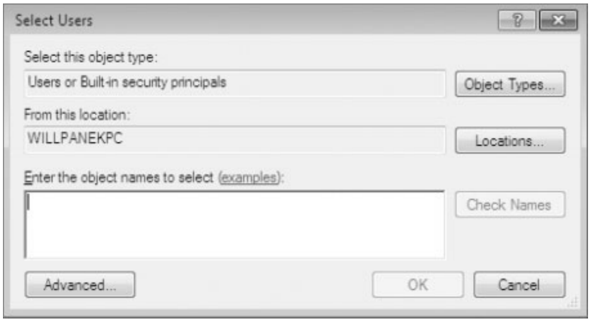
Executives

Description:

Members:
JAdams

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

**FIGURE 8.12**
The Select Users dialog box



Select this object type:
Users or Built-in security principals

From this location:
WILLPANEKPC

Enter the object names to select (examples):

To remove a member from the group, select the member in the Members list of the Properties dialog box and click the Remove button.

Perform the following steps to create new user accounts and then add these users to one of the groups you created in the previous steps:

1. Open the Admin Console MMC shortcut you created and expand the Local Users and Groups snap-in.
2. Create two new users: JDoe and DDoe. Deselect the User Must Change Password At Next Logon option for each user.
3. Expand the Groups folder.
4. Double-click the Data Users group.
5. In the Data Users Properties dialog box, click the Add button.

6. In the Select Users dialog box, type the username **JDoe**, then click OK. Click Add and type the username **DDoe**, then click OK.

7. In the Data Users Properties dialog box, you will see that the users have all been added to the group. Click OK to close the group's Properties dialog box.

Another task that might need to be completed is changing the name of a group, and we discuss this in the next section.

### Renaming Groups

Windows 7 provides an easy mechanism for changing a group's name. For example, you might want to rename a group because its current name does not conform to existing naming conventions, or you may need to rename a group because the group task or location may change.

For example, let's say we have a group called Sales but as the company grows, so do the office locations. We now might have to rename the group NHSales and then create other groups for the other locations.

#### Groups

As happens when you rename a user account, a renamed group keeps all of its properties, including its members and permissions.

To rename a group, right-click the group and choose Rename from the context menu. Enter a new name for the group and press Enter.

Perform the following steps to rename one of the groups you created in the previous steps:

1. Open the Admin Console MMC Desktop shortcut and expand the Local Users and Groups snap-in.

2. Expand the Groups folder.

3. Right-click the Data Users group and select Rename.

4. Rename the group to **App Users** and press Enter.

There might come a point when a specific group is no longer needed. In the next section we look at how to delete a group from the Local Users and Groups utility.

### Deleting Groups

If you are sure that you will never again want to use a particular group, you can delete it. Once a group is deleted, you lose all permissions assignments that have been specified for the group.

To delete a group, right-click the group and choose Delete from the context menu. You will see a warning that after a group is deleted, it is gone for good. Click the Yes button if you're sure you want to delete the group.

If you delete a group and give another group the same name, the new group won't be created with the same properties as the deleted group because as with users, groups are assigned unique SIDs at the time of creation.

Perform the following steps to delete the group that you created in the previous steps:

1. Open the Admin Console MMC shortcut you created and expand the Local Users and Groups snap-in.
2. Expand the Groups folder.
3. Right-click the App Users group and choose Delete.
4. In the dialog box that appears, click Yes to confirm that you want to delete the group.

Creating users and groups is one of the most important tasks that we as IT members can do. On a Windows 7 machine, creating users and groups is an easy and straightforward process.

Because most of the Windows 7 machines that you deal with will be part of a domain, you might need to create these users and groups as domain users. This process is discussed in detail in Chapter 12, ''Networking with Windows Server 2008.''

## The Bottom Line

**Understand user account types.** Windows 7 uses two basic account types: Administrator and Standard User. The Administrator account type provides unrestricted access to performing administrative tasks. Administrator accounts should be used only for performing administrative tasks and should not be used for normal computing tasks.

The Standard User type is the account type that should be applied for every user of the computer. Standard User accounts can perform most day-to-day tasks on the Windows 7 machine.

> **Master It** You are the administrator for a large computer company. You need to set up 20 Windows 7 machines and 20 local user accounts on those machines. When setting up the user accounts, what type of user account should these users have?

**Create accounts.** To create user accounts for your Windows 7 users, you have multiple options. To create local user accounts you can use the Local Users and Groups MMC snap-in, or you can use the User Accounts option in Control Panel. To create domain users accounts, you use Active Directory Users and Computers (see Chapter 12 for more information).

> **Master It** You are the administrator for a large computer company. You need to create 20 local users accounts for the 20 new Windows 7 machines that your company has just purchased. How would you accomplish this task?

**Configure accounts.** When you're configuring users' accounts, you deal with three main categories of properties: General, Member Of, and Profile.

The General tab contains the information you supplied when you set up the new user account, including any Full Name and Description information, the password options you selected, and whether the account is disabled.

The Member Of tab allows you to place this account into local groups on this Windows 7 machine. The Profile tab enables you to configure a user's Profile data, including user profile path, logon scripts, and home folder locations.

> **Master It** You are the administrator for a small pottery company. Your users are complaining that when they work on any machine that is not their own, the desktop settings are different. This is causing an issue for your users. What can you do to make sure that all users have their own desktop settings no matter which machine they are working on?

**Understand local groups.** Groups are a way to make sure that similar users get access to similar resources without having to add individual user accounts to each resource. Groups are an important part of network management.

Windows 7 includes built-in local groups, such as Administrators and Backup Operators. These groups already have all the permissions needed to accomplish specific tasks. Windows 7 also uses default special groups, which the system manages. Users become members of special groups based on their requirements for computer and network access.

You can create and manage local groups through the Local Users and Groups utility. The Local users and Groups snap-in allows you to add groups, change group membership, rename groups, and delete groups.

> **Master It** You are the administrator for a large organization. You have decided to set up local groups on all the Windows 7 machines so that all salespeople have access to the same resources. How do you accomplish this goal?