MCSE EXAM MATERIAL

▶ Professional
▶ Server
▶ Directory Services

EXAM OBJECTIVES

Professional ▶

Exam 70-210

- Configure and manage user profiles.
- Implement, configure, manage, and troubleshoot local user accounts.
    - Implement, configure, manage, and troubleshoot account settings.
    - Implement, configure, manage, and troubleshoot account policy.
    - Create and manage local users and groups.
    - Implement, configure, manage, and troubleshoot user rights.
- Implement, configure, manage, and troubleshoot local user authentication.
    - Configure and troubleshoot local user accounts.
    - Configure and troubleshoot domain user accounts.

Server ▶

Exam 70-215

- Configure and manage user profiles.
- Implement, configure, manage, and troubleshoot local accounts.
- Implement, configure, manage, and troubleshoot Account Policy.

Directory Services ▶

Exam 70-217

- Manage Active Directory objects.
    - Create and manage accounts manually or by scripting.

CHAPTER

9 Managing Users and Groups

I almost called this chapter "Everything You Always Wanted to Know About Users and Groups but Were Afraid Someone Would Explain to You in Great Detail." It's way too long a title, but it conveys the idea that this chapter is a comprehensive study of users and groups in a Windows 2000 environment. I'll start by explaining how user authentication works. Then I'll spend the rest of the chapter exploring user and group accounts. I'll take you through the steps involved in just about every local and domain user task you can think of, from creating and configuring user accounts to copying, renaming, and deleting user accounts. I'll also show you how to work with user profiles, account policies, and user rights, and spend some time explaining how to troubleshoot these features. Then I'll move on to groups, where I'll begin by explaining how to use local and built-in groups on the local computer. Finally, I'll discuss groups in Active Directory, including how to create, configure, and manage these groups.

Chapter Pre-Test

1. What is Kerberos V5?
2. What are the two Windows 2000 built-in user accounts?
3. What's the difference between a local user account and a domain user account?
4. What are roaming user profiles and mandatory user profiles?
5. What are the three major types of Windows 2000 account policies?
6. What's the difference between a security group and a distribution group?
7. What type of group has preset characteristics and is automatically created during the installation of Windows 2000?

Creating and Managing User Accounts

User accounts are records that contain unique user information, such as user name, password, and any logon restrictions. User accounts enable users to log on to Windows 2000 computers, and to access resources on the network.

There's a lot to know about creating and managing user accounts. In the following sections I'll explain the user authentication process and discuss the built-in user accounts. Then I'll show you how to create user accounts; how to configure and manage user account properties; and how to copy, rename, and delete user accounts. Finally, I'll explore user profiles, account policies, user rights, and several troubleshooting topics.

Understanding User Authentication

User authentication is the process of verifying a user's credentials for the purpose of determining whether the user is permitted to access a local computer or a network resource, such as a shared folder or shared printer. In Windows 2000, user authentication is performed by either the local computer (if the user logs on by using a local user account) or by a domain controller (if the user logs on by using a domain user account).

Windows 2000 supports three different authentication protocols:

- **Kerberos V5:** This protocol is an Internet standard authentication protocol that provides a higher level of security and faster, more efficient authentication than the Windows NT LAN Manager protocol. Kerberos V5 is the default protocol used between Windows 2000 computers when each of these computers is a member of a Windows 2000 domain. Kerberos V5 is not used, however, when the computers belong to Windows 2000 domains that are located in different forests.
- **Windows NT LAN Manager (NTLM):** This protocol enables users of Windows 95, Windows 98, and Windows NT client computers to be authenticated to Windows 2000 domains and network resources. This protocol is only available when Windows 2000 Active Directory is configured to operate in mixed-mode. This protocol is disabled when Windows 2000 Active Directory is configured to operate in native-mode.

- **Secure Sockets Layer/Transport Layer Security (SSL/TLS):** This protocol is primarily used to authenticate Internet users to secure Web sites. It can also be used to authenticate Internet users to Windows 2000 computers. This protocol requires the use of Certificate Services, and each user account must be mapped to an individual certificate.

CROSS-REFERENCE

I'll cover Certificate Services in more depth in Chapter 18.

There are two primary types of Windows 2000 authentication processes: interactive logon authentication and network authentication.

Interactive Logon Authentication

Interactive logon authentication is the process of verifying a user's credentials for the purpose of determining whether the user is permitted to log on to a local Windows 2000 computer.

Here's a basic description of what happens when a user logs on to a Windows 2000 computer. (Because Kerberos V5 is the default Windows 2000 authentication protocol, I assume that the Kerberos V5 protocol is used in this illustration.)

1. The user presses Ctrl+Alt+Delete, then enters a user name and password, and specifies whether he or she wants to log on to the local computer or to a domain.
2. If the user logs on to the local computer, the local Windows 2000 computer checks the user name and password against the information in its local user account database. If these items match, the computer logs the user on, and the authentication process is complete.

   If the user logs on to the domain, the local Windows 2000 computer converts the user's password into an encryption key. The local computer uses this encryption key to encrypt timestamp information. Then the local computer sends the user name and the encrypted timestamp information to a Windows 2000 domain controller, along with a request for user authentication.
3. The Windows 2000 domain controller (using the user name and the user's stored password from the Active Directory data store) unencrypts the timestamp information. If the unencryption process produces a

valid timestamp, the domain controller creates two Kerberos V5 tickets, encrypts these tickets by using the user's stored password as an encryption key, and sends the encrypted tickets back to the local Windows 2000 computer. One of these tickets, called the *logon session key,* contains the credentials the user needs to establish the logon session. The other ticket, called a *ticket-granting ticket* or a *user ticket,* is used to obtain additional Kerberos V5 tickets that enable the user to access network resources.

4. The local Windows 2000 computer (using the encryption key it created in Step 2) unencrypts the two Kerberos V5 tickets, and uses the logon session key to log the user on.

Network Authentication

Network authentication is the process of verifying a user's credentials for the purpose of determining whether the user is permitted to access network resources, such as a shared folder, a shared printer, or a network service.

Here's a high-level overview of what happens when a user attempts to access a network resource. (Because Kerberos V5 is the default Windows 2000 authentication protocol, I assume that the Kerberos V5 protocol is used in this example.)

1. The user attempts to access the network resource from the local Windows 2000 computer.

   The action the user takes to initiate access can take several forms. For example, the user could attempt to open a file stored on a network server from within an application, such as Microsoft Word. Or, the user could click Print within any application. There are numerous actions the user can take, but they all boil down to the user attempting to access a network resource.

2. The local Windows 2000 computer sends a Kerberos Ticket-Granting Service Request that includes the user's name, the name of the network resource the user wants to access, encrypted timestamp information, and the ticket-granting ticket (received when the user logged on) to a Windows 2000 domain controller.

3. The Windows 2000 domain controller unencrypts the timestamp information. If the unencryption process produces a valid timestamp, the domain controller uses the information in the Ticket-Granting

Service Request to create and encrypt a session key. This session key includes the user's authorization data (including user account and group membership information). Then the domain controller sends this encrypted session key to the local Windows 2000 computer.

4. The local Windows 2000 computer sends the encrypted session key to the network server that hosts the network resource that the user wants to access, along with a request for access to the resource.
5. The server that hosts the resource unencrypts the session key, and then checks the user's authorization data against the access control list (ACL) for the network resource. If the user has permission to access the resource in question, the server grants the user access to the resource.

Built-in User Accounts

There are two Windows 2000 built-in user accounts: Administrator and Guest. On nondomain controllers, the built-in user accounts are created automatically during the installation of Windows 2000. On a domain controller, the built-in user accounts are created automatically during the installation of Active Directory.

The Administrator user account has all of the rights and permissions needed to fully administer a Windows 2000 computer or a Windows 2000 domain. The Administrator account can be used to perform numerous tasks, such as creating and managing users and groups, managing file and folder permissions, and installing and managing printers and printer security.

The Administrator account, because of its powerful capabilities, can pose a security risk to your network if a nonauthorized user is able to guess the password for the account. For this reason, you should consider renaming the Administrator account. (I'll explain how to rename a user account later in this chapter.)

You can't delete the Administrator account. You also can't disable the Administrator account, nor can you remove this account from the Administrators local group. Incidentally, it's the Administrator account's membership in the Administrators local group that gives the Administrator account all of its rights and permissions.

The Guest account, which is disabled by default, is designed to permit limited access to network resources to occasional users who don't have their own user accounts. For example, a client visiting your office might want to connect a laptop computer to your network in order to print a document. Once the Guest account is enabled, the client can log on using this account. You can specify, in advance, which network resources are available to the Guest account by assigning the appropriate file, folder, and printer permissions to this account.

The Guest account does not require a password. If your network contains sensitive data, I recommend, for security reasons, that you leave the Guest account disabled. In this situation, instead of using the Guest account, you should establish a user account for each and every person who needs access to network resources.

You can't delete the Guest account, but you can rename it.

Creating User Accounts

Every person who uses the network on a regular basis should have a user account.

There are two kinds of user accounts: local user accounts and domain user accounts. *Local user accounts* enable users to log on to the local computer and to access that computer's resources. *Domain user accounts* enable users to log on to the domain and to access resources in the domain.

In order to create local user accounts, you must be a member of either the Administrators or Power Users group on the local computer. In order to create domain user accounts, you must be a member of either the Administrators or Account Operators group in the domain.

I'll show you how to create user accounts in just a minute, but before I do, I want to say a few words about naming conventions and passwords.

Naming Conventions

When you create user accounts, keep in mind a few simple rules for user names:

- User names (which are referred to as *user logon names* in Active Directory Users and Computers) can be from one to 20 characters long.

TIP

Windows 2000 allows you to enter *more* than 20 characters for a user name, but will only recognize the first 20.

- User names must be unique. A domain user name can't be the same as another user, group, or computer name within the domain. A local user name can't be the same as another user, group, or computer name within the local computer's account database.
- The following characters may *not* be used in user names:

  " / \ [ ] : ; | = , + * ? < >

  In addition, a user name can't consist entirely of spaces or periods.

If you have more than a few people in your organization, it's a good idea to plan your user account naming convention.

There are probably as many user account naming schemes as there are network administrators. Sometimes the overall length of a user name is limited to eight characters, so that the name is compatible with MS-DOS directory name limitations. While this eight-character limitation is common, it's certainly not mandatory, especially on most of today's networks. A few common naming conventions for user names include:

A. The first seven letters of the user's first name plus the first letter of the user's last name

B. The first letter of the user's first name plus the first seven letters of the user's last name

C. The user's initials plus the last four digits of the user's employee number

D. Various hybrid combinations of the preceding schemes

Table 9-1 shows how three user names would appear using the naming conventions described in A, B, and C.

TABLE 9-1 Common User Account Naming Conventions

Full Name	Scheme A	Scheme B	Scheme C
Nadine Smith	NadineS	NSmith	NS5500
Robert Jones	RobertJ	RJones	RJ1234
Jonathan Whitmore	JonathaW	JWhitmor	JW2266

In addition to choosing a naming convention, you should have a way to handle exceptions. It's quite common, for example, for two users to have the same first name and last initial, such as Mike Smith and Mike Sutherland. If your company uses the naming convention described in scheme A, you would need to resolve the potentially duplicate user names for these two employees. You could resolve the problem by assigning Mike Smith the user name of MikeS (assuming he was hired before Mike Sutherland), and assigning Mike Sutherland the user name of MikeSu.

Passwords

I'll just say a few words about passwords. Everyone knows that using passwords protects the security of the network, because only authorized users can log on.

When user accounts are created, you should have a plan for managing passwords. Will passwords be assigned and maintained by the network administrator? Or, will users choose their own passwords?

IN THE REAL WORLD

I normally recommend that the network administrator *not* maintain user passwords, because it can take an enormous amount of time. However, if a very high level of network security is required, the administrator may decide to assign user passwords of appropriate length and complexity.

When users maintain their own passwords, it's a good idea to remind them of a few password security basics:

- Don't use your own name or the name of a family member or pet as a password. (This is a common security loophole in most networks.)
- Never tell your password to anyone.
- Don't write your password on a sticky note and then stick it on your monitor. Other not-so-hot places to store your password are on or under your keyboard; in your top desk drawer; in your Rolodex; or in your briefcase, wallet, or purse.
- Use a sufficiently long password. I recommend using eight or more characters in a password. The longer the password, the more difficult it is to guess.
- Use a mix of uppercase and lowercase letters, numbers, and special characters. Remember, passwords are case-sensitive.
- If passwords are required to be changed regularly, don't use the same password with an incremental number at the end, such as Alan01, Alan02, Alan03, and so on. (Don't laugh. This may seem like common sense, but I've seen several network administrators actually do this.)

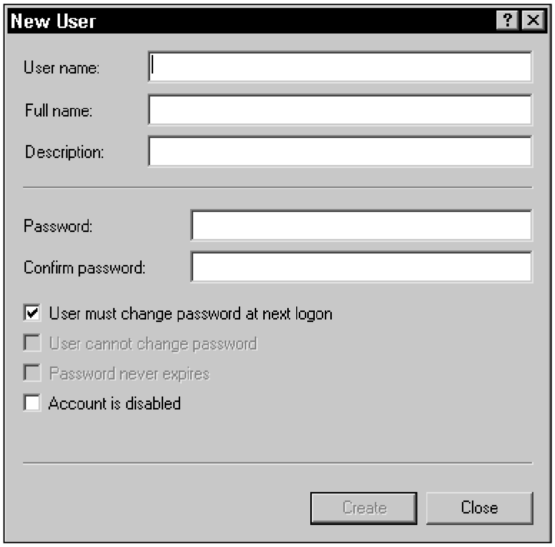
Creating Local User Accounts

You can use the Local Users and Groups tool in Computer Management to create local user accounts on a nondomain controller, as the following steps explain.

STEP BY STEP

CREATING A LOCAL USER ACCOUNT

1. From the desktop, right-click My Computer, and select Manage from the menu that appears.
2. In the Computer Management dialog box, click the + next to Local Users and Groups. Highlight the `Users` folder, and select Action ➪ New User.
3. The New User dialog box appears, as shown in Figure 9-1. Notice that by default the new user must change his or her password when he or she first logs on.



User name:

Full name:

Description:

Password:

Confirm password:

☑ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☐ Account is disabled

FIGURE 9-1 Creating a new user

Enter the user name, the person’s full name (this entry is optional), description (this could be a department, location, or job title – it is also optional) and password (also optional). Confirm the password by retyping it.

Accept the default selection of “User must change password at next logon” if you want the user to choose and enter a new password the first time the user logs on. If you don’t want the user to change his or her password the first time the user logs on, clear this check box.

STEP BY STEP *Continued*

If the “User must change password at next logon” check box is cleared, two additional check boxes become available. Select the “User cannot change password” check box if you – the network administrator – want to manage and assign user passwords. Select the “Password never expires” check box if you are configuring a user account for a Windows 2000 service to use when it logs on.

Select the check box next to “Account is disabled” if you are creating a user template. (I’ll cover user templates in the section titled “Copying User Accounts” later in this chapter.)

Click Create.

4. The New User dialog box reappears. Add additional users as necessary. When you are finished adding users, click Close.
5. The new user(s) is created, and appears in the right pane of the Computer Management dialog box.

Creating Domain User Accounts

To create domain user accounts in Active Directory, use Active Directory Users and Computers, as explained in the following steps.

STEP BY STEP

CREATING A DOMAIN USER ACCOUNT

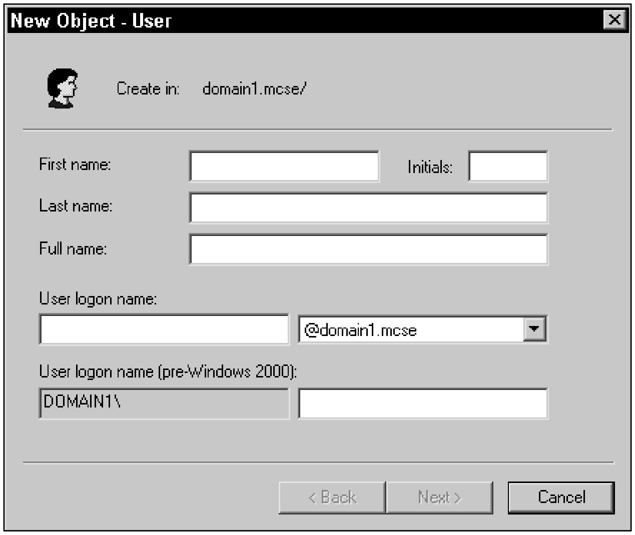
1. Start Active Directory Users and Computers. (Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.)
2. In the left pane of the Active Directory Users and Computers dialog box, click the + next to the name of the domain in which you want to create a domain user account. Notice the `Users` folder in the domain tree. This folder is the default container in which Windows 2000 places all users and many of the groups that it automatically creates when Active Directory is installed.

   If you have a relatively small organization, you may want to place your administrator-created user accounts in the `Users` folder, too, so that you can easily locate and administer all user accounts.

   Or, if you have a large organization and use organizational units (OUs) to administer groups of users, you can place each newly created user in the appropriate OU.

   Highlight the `Users` folder or the OU in which you want to create a domain user account, and select Action ➪ New ➪ User.
3. The New Object - User dialog box appears, as shown in Figure 9-2.

STEP BY STEP *Continued*



Create in: domain1.mcse/

First name: Initials:

Last name:

Full name:

User logon name: @domain1.mcse

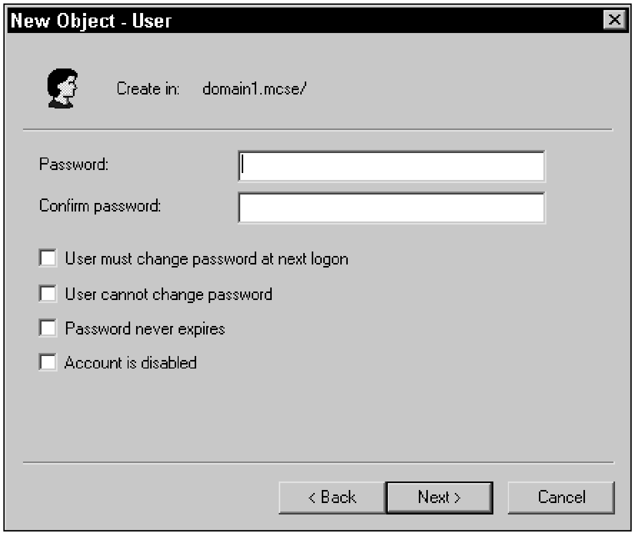
User logon name (pre-Windows 2000): DOMAIN1\

FIGURE 9-2 Creating a new domain user account

Enter the first name, middle initial, and last name of the new user in the appropriate text boxes. Windows 2000 automatically displays the full name based on the information you entered.

Enter a user logon name — this is the user name. Click Next.

4. The next New Object - User dialog box appears, as shown in Figure 9-3.



Create in: domain1.mcse/

Password:

Confirm password:

☐ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☐ Account is disabled

FIGURE 9-3 Configuring password options for a new domain user account

STEP BY STEP *Continued*

Enter the password for the new user account, and confirm the password by retyping it. (Entering a password is optional.)

There are four check boxes that can be selected in this dialog box, none of which are selected by default:

- **User must change password at next logon:** Select this check box if you want the user to choose and enter a new password the first time the user logs on.
- **User cannot change password:** Select this check box if you – the network administrator – want to manage and assign user passwords.
- **Password never expires:** Select this check box if you are configuring a user account for a Windows 2000 service to use when it logs on.
- **Account is disabled:** Select this check box if you are creating a user template. (I'll cover user templates in the section titled "Copying User Accounts" later in this chapter.)

Make the appropriate configurations in this dialog box, and then click Next.

5. In the next New Object - User dialog box, click Finish.
6. Windows 2000 creates the new user account, and displays it in the right pane of the Active Directory Users and Computers dialog box.

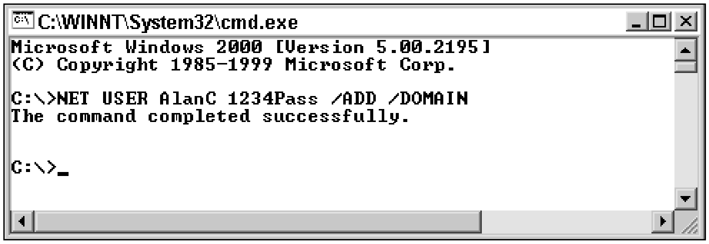
Using NET USER to Create User Accounts

You can also create user accounts by using a batch file or a script file in conjunction with the `NET USER` command-line utility. Using a batch file or a script file can be useful for automating the creation of user accounts, but this method is not widely used by administrators because it's typically easier to use the Windows 2000 graphical tools to create user accounts.

You can use Notepad (or your favorite text editor) to create the batch or script file. If you create a batch file, it should end with a `.bat` extension.

The `NET USER` command-line utility can also be used from the command line to manually create user accounts. Figure 9-4 shows how the `NET USER` command is used to create a new domain user account named AlanC with a password of 1234Pass.

Windows 2000 places domain user accounts created by using the `NET USER` command (either manually or by using a script) in the `Users` folder in the domain to which the administrator creating the user account is currently logged on.



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>NET USER AlanC 1234Pass /ADD /DOMAIN
The command completed successfully.


C:\>_
```

FIGURE 9-4 Using NET USER to create a new user

The syntax for the `NET USER` command is fairly complex. To view this command's syntax, type **net help user | more** at the command prompt, and press Enter.

Configuring and Managing User Account Properties

Once you create user accounts, you'll need to configure them. The numerous options that can be configured on user accounts are called user account properties.

In order to fully configure local user accounts, you must be a member of the Administrators group on the local computer. In order to fully configure domain user accounts, you must be a member of the Administrators group in the domain. Members of the Power Users group on the local computer and members of the Account Operators group in the domain can perform some, but not all, user configuration tasks.

Local user accounts have fewer configurable properties than domain user accounts, as the next sections illustrate.

Configuring Local User Accounts

You can use the same tool to view and configure local user account properties that you use to create local user accounts—the Local Users and Groups tool in Computer Management.

EXAM TIP

Both the Professional and Server exams test implementing, configuring, managing, and troubleshooting local user accounts. You should practice creating and configuring local user accounts until you've mastered these tasks.

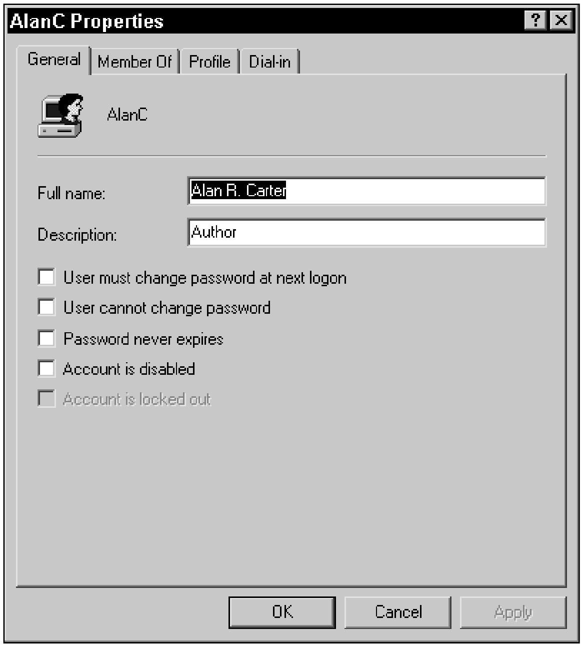
STEP BY STEP

ACCESSING AND CONFIGURING A LOCAL USER ACCOUNT'S PROPERTIES

1. From the desktop, right-click My Computer, and select Manage from the menu that appears.
2. In the Computer Management dialog box, click the + next to Local Users and Groups. Highlight the `Users` folder. In the right pane, double-click the user whose properties you want to configure. Or, you can right-click the user, and select Properties from the menu that appears.
3. The user's Properties dialog box appears. Configure the user's properties as necessary, and click OK.

The next several sections describe the tabs available in a local user account's Properties dialog box, and their many configurable options.

General On the General tab you can configure the local user's full name, description of the user account, and various password options, as shown in Figure 9-5. Notice the check box next to "Account is locked out."



Full name: Alan R. Carter

Description: Author

☐ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☐ Account is disabled

☐ Account is locked out

FIGURE 9-5 Configuring a local user account's general properties

Also notice that the "Account is locked out" check box is grayed out. If the account has been locked out (due to too many unsuccessful logon attempts), this check box will be checked. To unlock a locked account, you need to clear this check box.

Member Of On the Member Of tab you can configure the local user's membership in the local groups on the local computer. Assigning users to groups is an efficient way to manage permissions for multiple users. Click Add to make the user account a member of a group, and click Remove to remove the user account from a group. By default, all users are members of the Users local group.

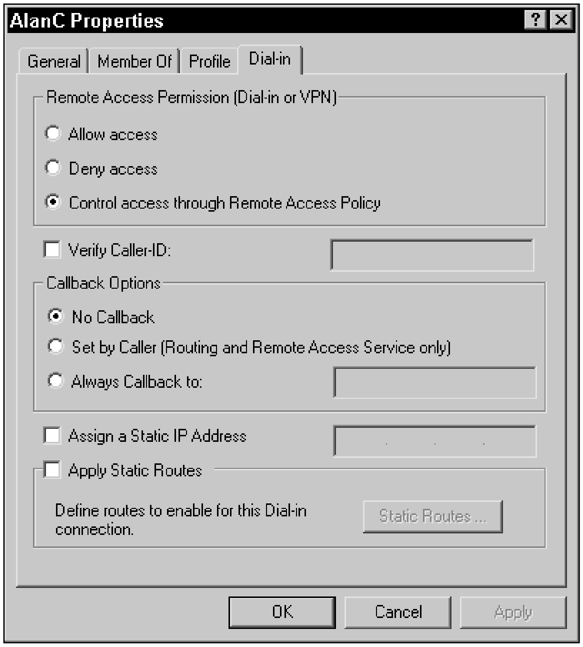
Profile The Profile tab is used to configure the local user's environment. On this tab you can specify a local or network path to the user's `Profile` folder. A user's profile contains the user's unique desktop settings, such as screen color, screen saver, desktop icons, fonts, and so on. The default location for a user's profile is the `C:\Documents and Settings\`*`user_name`* folder. If no path is entered on this tab, Windows 2000 uses the default location. (I'll cover managing user profiles in more detail later in this chapter.)

On the Profile tab you can also specify a network or local path to the user's `Home` folder, and specify the name of the user's logon script file, if a logon script is used. A logon script is a batch file that is run each time a user logs on. Logon scripts for local user accounts must be stored in the *`SystemRoot`*`\System32` folder. Logon scripts are commonly used to automatically connect network drives and printers, and to install and maintain certain types of software, such as the Systems Management Server (SMS) client.

Dial-in On the Dial-in tab you can configure numerous dial-in properties for the local user account. This tab is only available on Windows 2000 Server/Advanced Server computers. Figure 9-6 shows the Dial-in tab.

CROSS-REFERENCE

I'll discuss configuring dial-in properties extensively when I cover remote access in Chapter 17.



AlanC Properties

Remote Access Permission (Dial-in or VPN)

○ Allow access

○ Deny access

● Control access through Remote Access Policy

□ Verify Caller-ID:

Callback Options

● No Callback

○ Set by Caller (Routing and Remote Access Service only)

○ Always Callback to:

□ Assign a Static IP Address

□ Apply Static Routes

Define routes to enable for this Dial-in connection.

FIGURE 9-6 Configuring a local user account’s dial-in properties

Configuring Domain User Accounts

You use the same tool to view and configure domain user account properties that you use to create domain user accounts — Active Directory Users and Computers.

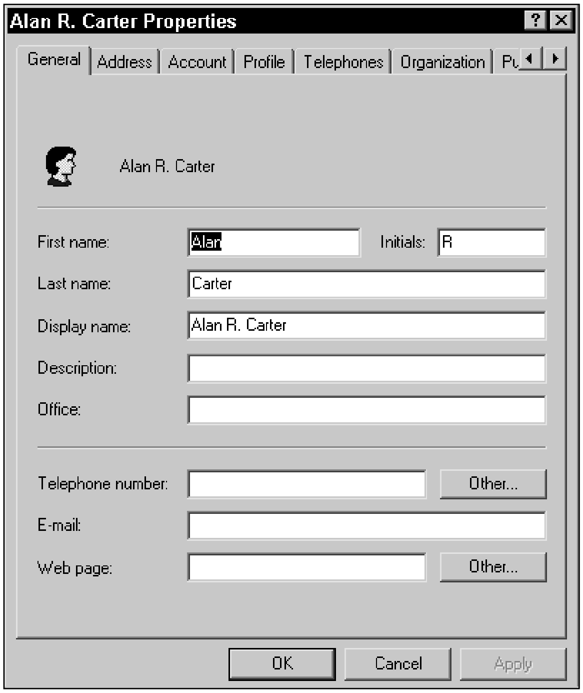
STEP BY STEP

ACCESSING AND CONFIGURING A DOMAIN USER ACCOUNT’S PROPERTIES

1. Start Active Directory Users and Computers. (Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.)
2. In the left pane of the Active Directory Users and Computers dialog box, click the + next to the name of the domain that contains the user account you want to configure. Highlight the `Users` folder or the OU that contains the user account you want to configure. In the right pane, double-click the user account you want to configure. Or, you can right-click the user account, and select Properties from the menu that appears.
3. The user’s Properties dialog box appears. Configure the user’s properties as necessary, and click OK.

The next several sections describe the many tabs available in a domain user account's Properties dialog box, and their many configurable options.

General On the General tab you can configure the domain user's name and contact information, as shown in Figure 9-7.



Alan R. Carter Properties

Alan R. Carter

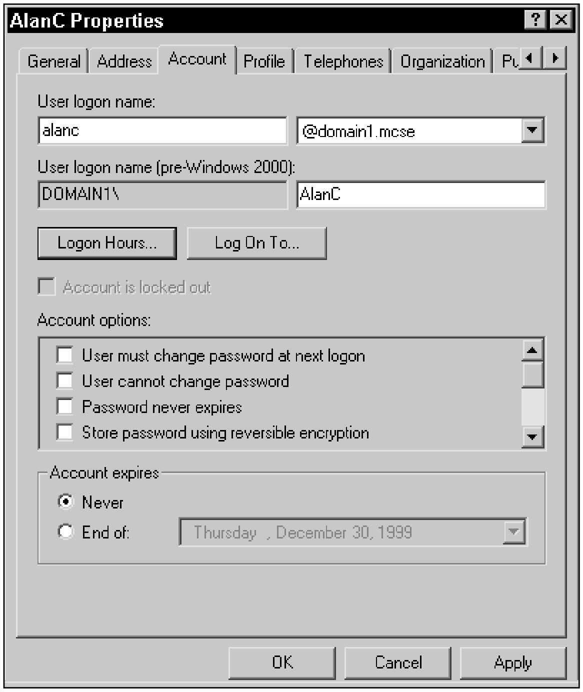
First name: Alan
Initials: R
Last name: Carter
Display name: Alan R. Carter
Description:
Office:
Telephone number:
E-mail:
Web page:

FIGURE 9-7 Configuring a domain user account's general properties

On this tab, you can change the user's first name, last name, and display name. You can also add a description of the user account and the location of the user's office. Finally, you can configure the user's telephone number, e-mail address, and Web page address.

Address On the Address tab, you can configure detailed mailing and/or physical address information for the domain user. The configurable options on this tab are self-explanatory.

Account On the Account tab, you can configure the domain user's logon name, logon hours, computers the user can log on to, password and other account options, and account expiration information, as shown in Figure 9-8. Notice the check box next to "Account is locked out."



User logon name: alanc @domain1.mcse

User logon name (pre-Windows 2000): DOMAIN1\ AlanC

□ Account is locked out

Account options:

□ User must change password at next logon
□ User cannot change password
□ Password never expires
□ Store password using reversible encryption

Account expires
● Never
○ End of: Thursday , December 30, 1999

FIGURE 9-8 Configuring account properties for a domain user

Also notice that the "Account is locked out" check box is grayed out. If the account has been locked out (due to too many unsuccessful logon attempts), this check box will be checked. To unlock a locked account you need to clear this check box.

There are ten options you can select in the "Account options" section of this tab:

- **User must change password at next logon:** Select this option if you want the user to choose a new password the next time the user logs on.
- **User cannot change password:** Select this option if you want to manage the user's password, rather than having the user choose his or her own password.
- **Password never expires:** Select this option if you are configuring a user account for a Windows 2000 service to use when it logs on.
- **Store password using reversible encryption:** Select this option if this user will be logging on to the domain from an Apple computer, because Apple computers use a different type of password encryption than Windows 2000 computers use.

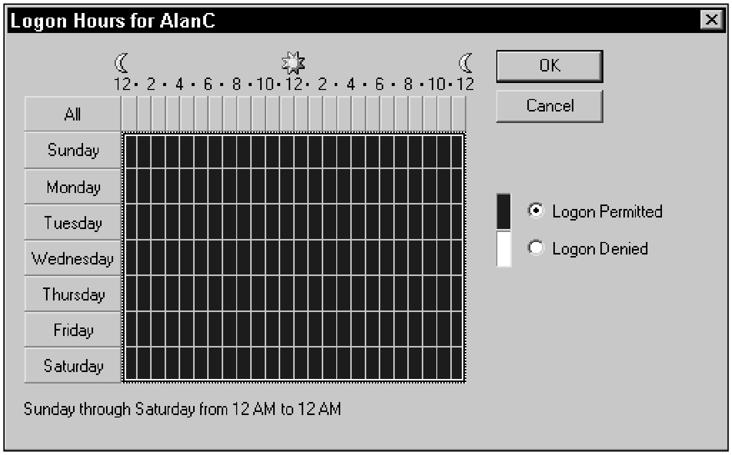
- **Account is disabled:** Select this option if the user account will be used as a user template.
- **Smart card is required for interactive logon:** Select this option if you want to require the user to use a smart card and pin number in order to log on.
- **Account is trusted for delegation:** Select this option if you want the user to be able to delegate administrative authority for a portion of the domain.
- **Account is sensitive and cannot be delegated:** Select this option if you want to prevent administrative authority for this user account from being delegated.
- **Use DES encryption types for this account:** Select this option if you want to use DES encryption for this account instead of standard Windows 2000 encryption.
- **Do not require Kerberos preauthentication:** Select this option if the user will be logging on to the domain from a computer that uses an operating system other than Windows 2000, and this other operating system supports the Kerberos protocol but doesn't support Kerberos preauthentication.

You can also set account expiration on the Account tab. There are two options on this tab: Never and "End of," where you specify the exact date the user account will expire. Never is often selected when the user is a permanent employee of the company, or when the account is used by a Windows 2000 service when it logs on. "End of" is often selected for temporary employees or contractors, so they can no longer access the network when their term of employment or contract has expired. When you select "End of," the user account expires at midnight on the date specified in the drop-down list box.

There are two other important configurations you can make on this tab:

- Logon Hours
- Log On To

Logon Hours specify the hours that a user is permitted to log on to the domain. Click Logon Hours to configure these hours. The Logon Hours for a specific user, AlanC, is shown in Figure 9-9. Notice that by default all hours are available for logon.



● Logon Permitted
○ Logon Denied

Sunday through Saturday from 12 AM to 12 AM

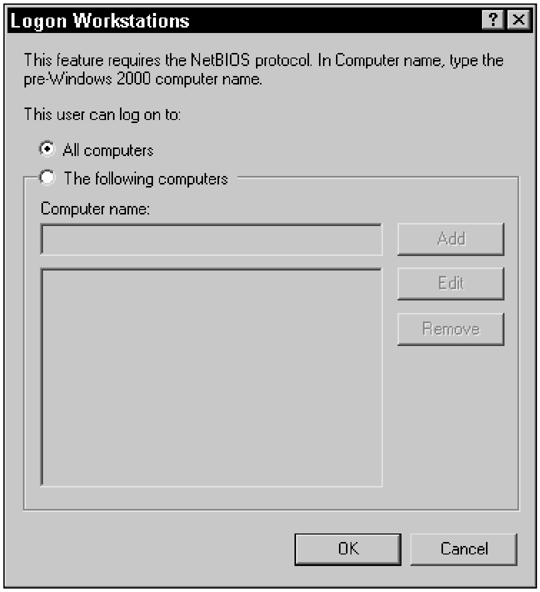
FIGURE 9-9 Configuring logon hours

It's a common practice to prevent users from logging on during certain hours of the day, such as the hours when a backup is being performed. To modify the user's logon hours, use your mouse to highlight the hours you *don't* want the user to be able to log on, and select the Logon Denied option. Or, you can use your mouse to highlight the entire graph, select the Logon Denied option, highlight the hours you *want* the user to be able to log on, and then select the Logon Permitted option.

Restricting a user's logon hours does not disconnect a user from a domain when the user's logon hours expire. A logon hours restriction only *prevents* a user from logging on to the domain during the specified restricted hours. If you want to automatically log off all users (from the domain controller) when their logon time expires, you must enable this option in Local Policies – Security Options by using the Domain Security Policy tool. (I'll cover using Domain Security Policy later in this chapter.)

The Log On To command button enables you to specify which computers a user is permitted to log on to. Click Log On To to specify these workstations. The Logon Workstations dialog box is shown in Figure 9-10. Notice that by default the user is permitted to log on to all computers.

If you want to specify which computers a user can log on to, select "The following computers" option, then click Add to add specific computers to a list.



Logon Workstations

This feature requires the NetBIOS protocol. In Computer name, type the pre-Windows 2000 computer name.

This user can log on to:

● All computers

○ The following computers

Computer name:

FIGURE 9-10 Specifying the workstations a user can log on to

TIP

The Logon Workstations feature requires the NetBIOS protocol, and is primarily designed to restrict access to non-Windows 2000 computers that rely on NetBIOS. If you have removed NetBIOS from your Windows 2000 client computers, this feature won't work correctly.

Profile The Profile tab is used to configure the domain user's environment. On this tab you can specify a local or network path to the user's `Profile` folder. The default location for a user's profile is the `C:\Documents and Settings\`*`user_name`* folder on the computer the user logs on to. If no path is entered on this tab, Windows 2000 uses the default location. (I'll cover managing user profiles in more detail later in this chapter.)

On the Profile tab you can also specify a network or local path to the user's `Home` folder, and specify the name of the user's logon script file, if a logon script is used. Logon scripts for domain user accounts must be stored in the `NETLOGON` share on a domain controller. By default, the `NETLOGON` share is located in the *`SystemRoot`*`\SYSVOL\sysvol\`*`domain_name`*`\SCRIPTS` folder on each domain controller in the domain. Windows 2000 automatically replicates all information in the `SYSVOL` folder, including the `NETLOGON` share, to all domain controllers in the domain.

Telephones On the Telephones tab, you can specify detailed telephone information for the domain user, including home number, pager number, mobile number, fax number, and so on. The configurable options on this tab are self-explanatory.

Organization On the Organization tab, you can specify detailed personnel information for the domain user, including the user's title, department, company, manager's name, and so on. The configurable options on this tab are self-explanatory.

Published Certificates On the Published Certificates tab, you can add or remove X509 (Internet) certificates that have been issued to the domain user.

CROSS-REFERENCE

I'll cover Certificate Services in Chapter 18.

This tab is only present after you select View ➪ Advanced Features in the Active Directory Users and Computers dialog box.

Member Of On the Member Of tab you can configure the user's membership in groups in the domain. Click Add to make the domain user account a member of a group in the user's domain, and click Remove to remove the user account from a group in the user's domain. By default, all domain users are members of the Domain Users global group.

The Member Of tab also has an option to set a primary group for the user account. Windows 2000 doesn't require the use of primary groups, but users of Apple computers who access files on a Windows 2000 Server computer and users of Windows 2000 computers who run POSIX-compliant applications do require certain file ownership and permissions settings that a primary group provides. The default primary group is the Domain Users global group.

Dial-in On the Dial-in tab you can configure numerous dial-in properties for the domain user account. This Dial-in tab is identical to the Dial-in tab for a local user account, which was shown in Figure 9-6.

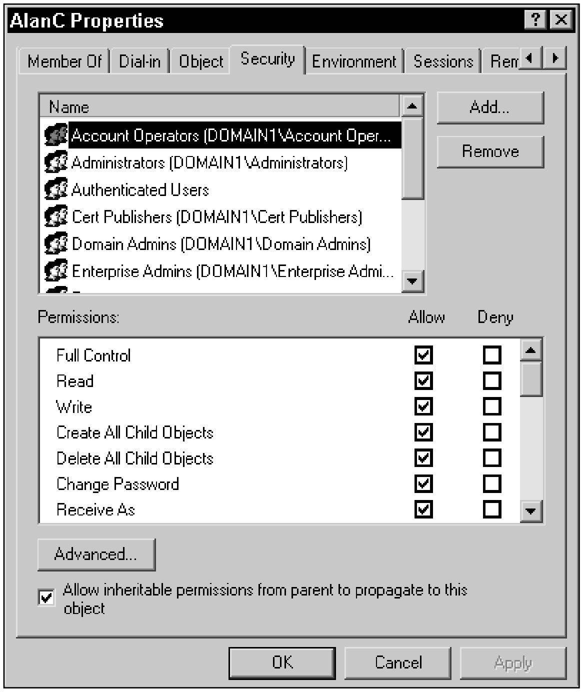
CROSS-REFERENCE

I'll discuss configuring dial-in properties extensively when I cover remote access in Chapter 17.

Object On the Object tab you can view limited information about the domain user account object, including the object's class, the date the user account was created, the date the user account was last modified, and so on. No configurations are possible on this tab. In addition, this tab is only present after you select View ➪ Advanced Features in the Active Directory Users and Computers dialog box.

Security On the Security tab you can specify the users and groups that are permitted to view or modify the properties of the domain user account. This tab is only present after you select View ➪ Advanced Features in the Active Directory Users and Computers dialog box.

The Security tab is shown in Figure 9-11. Notice the "Allow" and "Deny" check boxes for the various permissions listed.



Name
Account Operators (DOMAIN1\Account Oper...
Administrators (DOMAIN1\Administrators)
Authenticated Users
Cert Publishers (DOMAIN1\Cert Publishers)
Domain Admins (DOMAIN1\Domain Admins)
Enterprise Admins (DOMAIN1\Enterprise Admi...

Permissions:	Allow	Deny
Full Control	☑	□
Read	☑	□
Write	☑	□
Create All Child Objects	☑	□
Delete All Child Objects	☑	□
Change Password	☑	□
Receive As	☑	□

☑ Allow inheritable permissions from parent to propagate to this object

FIGURE 9-11 The Security tab

In the Name box, users and groups that have some sort of permission to view or modify one or more properties of this user are listed. You can use the Add and Remove command buttons to add and remove users and groups to and from the Name box.

You can set permissions on any user or group for this user by highlighting the user or group in the Name box and then selecting permissions in the Permissions box.

CROSS-REFERENCE

Setting permissions is covered extensively in the “Setting Permissions on Active Directory Objects” section in Chapter 8.

Environment, Sessions, Remote Control, and Terminal Services Profile On these four tabs you can configure various options for this domain user when the user logs on to and uses a Terminal Services session.

CROSS-REFERENCE

I’ll discuss Terminal Services (and the settings on these tabs) in Chapter 20.

Using Users and Passwords to Manage User Accounts

On Windows 2000 Professional computers, there is an additional tool you can use to manage local and domain user accounts — it’s called Users and Passwords, and it’s a Control Panel application. To use Users and Passwords, you must be a member of the Administrators group on the local computer.

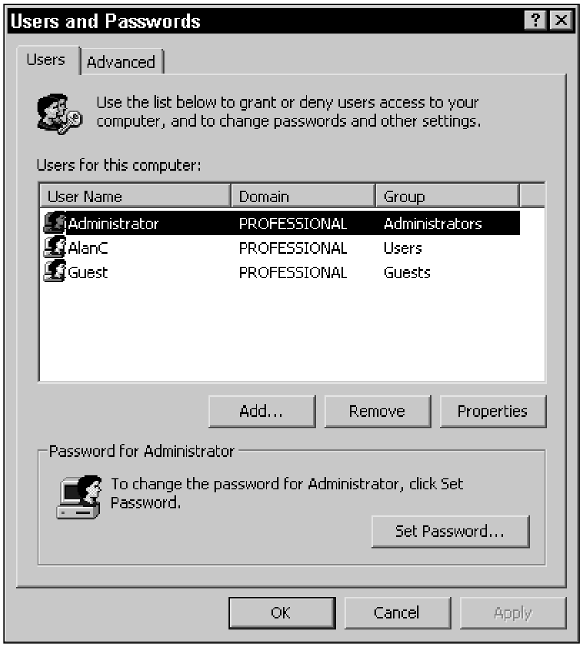
The Users and Passwords application enables you to manage users and passwords for the local computer. In this application you can grant or deny local (or domain) users access to the local computer, change passwords, manage certificates, access the Local Users and Groups tool in Computer Management, and configure whether local users are required to press Ctrl+Alt+Delete before logging on.

To start Users and Passwords on your Windows 2000 Professional computer, select Start ➪ Settings ➪ Control Panel, then double-click Users and Passwords. Figure 9-12 shows the Users and Passwords dialog box. Notice the list of users who are currently permitted to access this computer.

Also notice the three columns in the “Users for this computer” box: User Name, Domain, and Group. *User Name* is the user account name of each user who is permitted to access this computer. *Domain* refers to the location of the user account named in the first column, and it will be either the name of the local Windows 2000 Professional computer or the name of a Windows 2000 domain. (The Domain column only appears on Windows 2000 Professional computers that are members of a domain.)

Group is the name of the local group on the Windows 2000 Professional computer to which the user named in the first column belongs.

Click Add to add an *existing* user to the "Users for this computer" box.



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

Users for this computer:

User Name	Domain	Group
Administrator	PROFESSIONAL	Administrators
AlanC	PROFESSIONAL	Users
Guest	PROFESSIONAL	Guests

To change the password for Administrator, click Set Password.

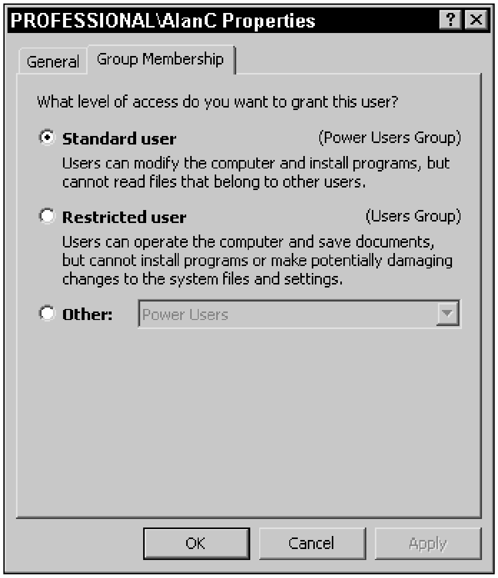
FIGURE 9-12 Users and Passwords

TIP

You can't use the Add command button to create new users.

Click Remove to remove a user from the "Users for this computer" box. If you highlight a local user in the "Users for this computer" box and click Remove, the user is deleted. If you highlight a domain user in the "Users for this computer" box and click Remove, the domain user is not deleted, but is denied access to this computer and is removed from the "Users for this computer" box.

To view or modify a user's properties or group memberships, highlight the user in the "Users for this computer" box and click Properties. If the user you highlighted is a local user, you can configure the user's name, full name, description, and group membership. For domain users, you can only configure group membership. The Group Membership tab is shown in Figure 9-13. Notice the three options in this dialog box.



What level of access do you want to grant this user?

● **Standard user** (Power Users Group)
Users can modify the computer and install programs, but cannot read files that belong to other users.

○ **Restricted user** (Users Group)
Users can operate the computer and save documents, but cannot install programs or make potentially damaging changes to the system files and settings.

○ **Other:** Power Users

FIGURE 9-13 Configuring group membership

On the Group Membership tab you can make the highlighted user a member of any group on the local computer. The options you can select from are:

- **Standard user:** Select this option if you want to make the user a member of the Power Users Group on the local computer. Members of this group can modify the computer and install programs, but can't read other users' files. This is the recommended setting for most environments.
- **Restricted user:** Select this option if you want to make the user a member of the Users Group on the local computer. Members of this group can log on to and use the local computer, can modify and save their own documents, but can't install programs or modify computer system settings. This is the recommended setting for high-security environments.
- **Other:** Select this option if you want to make the user a member of any other group on the local computer, such as Administrators, Backup Operators, and so on.

You can also use Users and Passwords to change the password for any *local* user listed in the "Users for this computer" box. To change a password, highlight the local user in the "Users for this computer" box, click Set

Password, type in (and confirm) the new user password in the Set Password dialog box, and then click OK.

On the Advanced tab in the Users and Passwords dialog box you can manage certificates, access the Local Users and Groups tool in Computer Management, and configure whether local users are required to press Ctrl+Alt+Delete before logging on.

Copying User Accounts

Sometimes the easiest way to create a new user account is to copy an existing user account. There are basically two ways to accomplish this:

- You can copy any existing user account that has properties and group memberships that are similar to the desired properties and group memberships for the new user account.
- You can create a new user account that will be used as a template to create multiple user accounts with the same set of account properties and group memberships.

TIP

Only domain user accounts can be copied—local user accounts can't be copied.

For example, suppose that you want to create a domain user account to be used by an employee who will administer the network. You want this user account to have all of the capabilities of the Administrator account, so you decide to copy the Administrator account. When a user account is copied, all properties of the user account, including its group memberships, are copied to the new user account with the exception of the user name, full name, password, logon hours, address and telephone information, organization information, the "Account is disabled" option, and user rights and permissions.

You can use Active Directory Users and Computers to copy user accounts.

STEP BY STEP

COPYING A USER ACCOUNT

1. Start Active Directory Users and Computers. (Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.)
2. In the left pane of the Active Directory Users and Computers dialog box, click the + next to the name of the domain that contains the user account you want to copy. Highlight the `Users` folder or OU that contains this user. In the right pane of the dialog box, right-click the name of the user you want to copy, and select Copy from the menu that appears.
3. In the Copy Object - User dialog box, fill in the requested information for the new user account that is being created by copying an existing user account. Enter the new user's first name, middle initial, last name, and user logon name. Click Next.
4. In the next Copy Object - User dialog box, enter the password for the new user account, and confirm the password by retyping it. (Entering a password is optional.) Select one or more appropriate password configuration options, then click Next.
5. In the next Copy Object - User dialog box, click Finish.
6. Windows 2000 creates the new user account, and displays it in the right pane of the Active Directory Users and Computers dialog box.

Suppose, instead, that you are setting up a new network and need to create multiple new user accounts for the accountants at a large CPA firm. All of the accountants at this firm have similar network access needs, and their user accounts will have substantially similar properties and group memberships. You can create a new user account, named Acct_Template, to use as a template to create these new user accounts.

To create a new user account that will be used as a template, follow the steps presented earlier in this chapter under "Creating a domain user account." When you create the new user account, assign the user account a name that indicates the type of user account this template will be used to create, such as Acct_Template for the accountants in the previous example. Configure the template user account's properties and group memberships to match the requirements of the user accounts you will create using this template.

TIP

When you create a user account to be used as a template, I recommend that you select the "Account is disabled" check box on the Account tab so that no one can log on using this account.

To use a template, copy it to create a new user account. All properties and group memberships of the template user account are copied to the new user account with the exception of the user name, full name, password, logon hours, address and telephone information, organization information, the "Account is disabled" option, and user rights and permissions.

Renaming and Deleting User Accounts

Occasionally you may want to rename or delete a user account.

Renaming a user account doesn't affect any of the user account's properties, except for its name. The user account, after it is renamed, retains all of its properties, including group memberships, permissions, and user rights. You might want to rename a user account when a new staff member replaces an employee who has left the company.

You can rename both local and domain user accounts, as the following steps explain.

STEP BY STEP

RENAMING A LOCAL USER ACCOUNT

1. From the desktop, right-click My Computer, and select Manage from the menu that appears.
2. In the Computer Management dialog box, click the + next to Local Users and Groups. Highlight the `Users` folder. In the right pane, right-click the user account you want to rename, and select Rename from the menu that appears.
3. Type in a new name for the user account, and press Enter. The user account is renamed.

RENAMING A DOMAIN USER ACCOUNT

1. Start Active Directory Users and Computers. (Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.)

STEP BY STEP *Continued*

2. In the left pane of the Active Directory Users and Computers dialog box, click the + next to the name of the domain that contains the user account you want to rename. Highlight the `Users` folder or OU that contains this user account. In the right pane of the dialog box, right-click the name of the user you want to rename, and select Rename from the menu that appears.
3. Type in a new name for the user account, and press Enter.
4. The Rename User dialog box appears. Fill in the requested information, including the user's first name, last name, and user logon name. (This is the information about the user who will use this user account from this point on.) Click OK. The user account is renamed.

Deleting a user account is just what it sounds like—the user account is permanently removed, and all of its group memberships, permissions, and user rights are lost. Normally you would only delete a user account when you never plan to use the account again.

When you delete a user account, the SID associated with the account is marked as deleted. If you later create a new account with the same name, A new SID will be associated with the account. For this reason, the new account won't have the same privileges as the old, deleted account.

The two built-in accounts, Administrator and Guest, can't be deleted, although they can be renamed.

You can delete both local and domain user accounts, as the following steps explain.

STEP BY STEP

DELETING A LOCAL USER ACCOUNT

1. From the desktop, right-click My Computer, and select Manage from the menu that appears.
2. In the Computer Management dialog box, click the + next to Local Users and Groups. Highlight the `Users` folder. In the right pane, right-click the user account you want to delete, and select Delete from the menu that appears.
3. A dialog box appears, asking if you're sure you want to delete the user account. Click Yes to delete the user account. The user account is deleted.

STEP BY STEP *Continued*

DELETING A DOMAIN USER ACCOUNT

1. Start Active Directory Users and Computers. (Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.)
2. In the left pane of the Active Directory Users and Computers dialog box, click the + next to the name of the domain that contains the user account you want to delete. Highlight the `Users` folder or OU that contains this user account. In the right pane of the dialog box, right-click the name of the user you want to delete, and select Delete from the menu that appears.
3. A dialog box appears, asking if you're sure you want to delete the user account object. Click Yes to delete the user account. The user account is deleted.

Managing User Profiles

A *user profile* is a folder that contains a collection of settings and options that specify a user's desktop and all other user-definable settings for a user's work environment. Both users and administrators can benefit from user profiles.

Benefits to users include:

- When a user logs on, the same desktop is displayed as when the user last logged off. This is because when a user makes changes to his or her desktop or work environment during the time the user is logged on, these settings are saved to the user's profile folder at logoff.
- When a computer has more than one user, a customized desktop is displayed for each user at logon.
- Roaming user profiles can be saved on a Windows 2000 Server computer, and thereby apply to a user no matter which Windows 2000 computer on the network the user logs on at.

Benefits to administrators include:

- Administrators can develop and assign user profiles that are customized, so each user has a desktop and work environment that complies with established company standards, and can assign user profiles that are suitable for the tasks that each user needs to perform.

- If desired or necessary, administrators can forcibly prevent certain users from permanently changing any of their desktop or work environment settings by assigning them mandatory user profiles.
- User profiles make it possible for administrators to assign common program items and shortcuts to all users by customizing the `All Users` profile folder.

EXAM TIP

User profiles cover a lot of ground, and are tested on both the Professional and Server exams. Every heading in this section is fair game, so spend as much time as it takes for you to be comfortable with all of the nuances of user profiles.

In the following sections I'll discuss the contents of a user profile, how a user profile is created, customizing the local and domain-wide `Default User` profile folder, customizing the `All Users` profile folder, roaming and mandatory user profiles, and deleting user profiles.

Contents of a User Profile

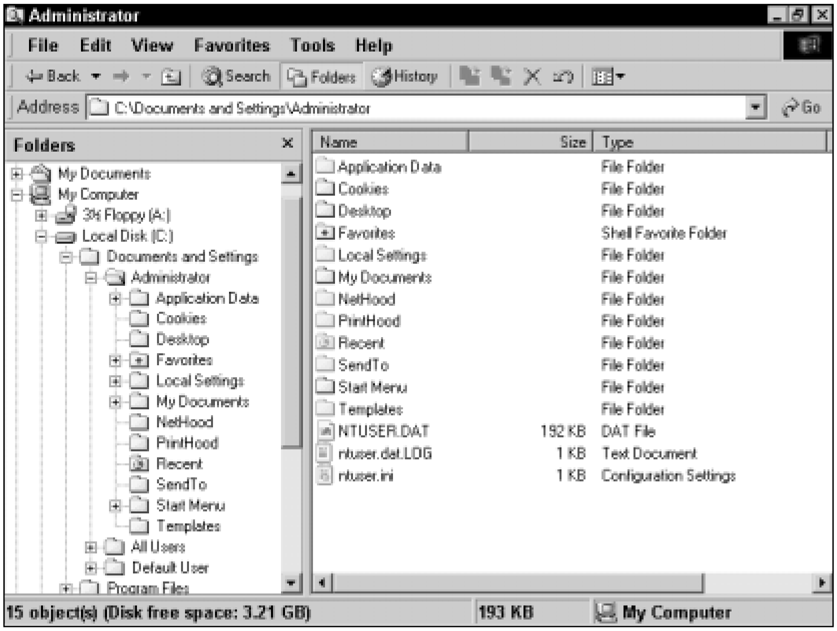
Various settings are saved in a user profile. The contents of a user profile include:

- All user-specific settings for Windows Explorer, Notepad, Paint, HyperTerminal, Clock, Calculator, and other built-in Windows 2000 applications
- User-specific desktop settings, including screen saver, background color, background pattern, wallpaper, and other display settings
- User-specific settings for applications written to run on Windows 2000
- User-specific settings for network drive and printer connections
- User-specific settings for the Start menu, including program groups, applications, and recently accessed documents

The default location for a user's profile is the `C:\Documents and Settings\`*`user_name`* folder on the Windows 2000 computer the user logs on to. Each user's profile is stored in a separate folder named after the user's account. For example, the Administrator's user profile is stored in the `C:\Documents and Settings\Administrator` folder. Figure 9-14 shows, in Windows Explorer, the location and contents of the Administrator's profile folder.

TIP

All user profiles have virtually the same contents as those shown for the Administrator.



C:\Documents and Settings\Administrator

Name	Size	Type
Application Data		File Folder
Cookies		File Folder
Desktop		File Folder
Favorites		Shell Favorite Folder
Local Settings		File Folder
My Documents		File Folder
NetHood		File Folder
PrintHood		File Folder
Recent		File Folder
SendTo		File Folder
Start Menu		File Folder
Templates		File Folder
NTUSER.DAT	192 KB	DAT File
ntuser.dat.LOG	1 KB	Text Document
ntuser.ini	1 KB	Configuration Settings

15 object(s) (Disk free space: 3.21 GB) 193 KB My Computer

FIGURE 9-14 Contents of the Administrator's profile folder

Note in Figure 9-14 that there are several subfolders and files contained in the Administrator's profile folder. Table 9-2 lists and describes each of these folders and files. All users' profile folders (not just the Administrator's) contain the folders and files listed in Table 9-2.

TABLE 9-2 Windows 2000 User Profile Folder Contents

Folder or File	Description
`Application Data`	This folder contains any user-specific application data that an application vendor has chosen to store in it. For example, a word processing application could store the user's custom dictionary in this subfolder.
`Cookies`	This folder contains cookies, which are files stored on the user's computer that provide customization of Internet or intranet Web sites.
`Desktop`	This folder contains all shortcuts, files, and folders stored on the user's desktop.

Folder or File	Description
Favorites	This folder contains shortcuts from the user's Favorites folder in various applications. For example, when you add an Internet site to your Favorites folder in Internet Explorer, a shortcut to that site is created in this folder.
FrontPageTempDir	This folder is only present in user profiles located on Windows 2000 Server computers. This folder contains temporary files created by using Microsoft FrontPage.
Local Settings	This folder contains several folders commonly used by Internet Explorer (and other Internet applications), including Application Data, History, Temp, and Temporary Internet Files.
My Documents	This folder contains user-created documents. It is the default location for saving user-created documents in most applications.
NetHood	This folder contains any shortcuts a user has created to network servers or shared folders. These shortcuts are displayed in the My Network Places dialog box.
PrintHood	This folder can contain shortcuts to network printers. These shortcuts are displayed in the Printers dialog box.
Recent	This folder contains shortcuts to document files the user has recently accessed. These shortcuts can be displayed by selecting Start ➪ Documents.
SendTo	This folder contains shortcuts to folders, briefcases, mail, the computer's floppy drive, My Documents, and so on. These shortcuts are displayed when a user right-clicks any file or folder, and then selects Send To from the menu that appears.
Start Menu	This folder contains the Programs folder from a user's Start menu, and any additional shortcuts to programs that the user has created in the Start Menu folder or any of its subfolders. These shortcuts are displayed in the Start menu, or in the Programs folder in the Start menu, depending on where the shortcut was created.
Templates	This folder contains application templates.
NTUSER.DAT	This file contains all of the registry settings that are specific to a user account. When a user logs on, the settings in this file are copied to the HKEY_CURRENT_USER registry settings on the local computer.
ntuser.dat.LOG	This file is used by Windows 2000 to recover the user's original NTUSER.DAT file if an error occurs while updating the NTUSER.DAT file.
ntuser.ini	This file contains settings that determine the components of a user's roaming user profile that are *not* copied to the server each time the user logs off.

Understanding How a User Profile Is Created

When a user logs on to a Windows 2000 computer, Windows 2000 checks to see if a user profile for that user exists on the local computer. If a user profile exists on the local computer, Windows 2000 uses the existing user profile. If no profile exists, Windows 2000 automatically creates a new user profile for the user and stores that profile on the local computer.

Windows 2000 implements user profiles on a computer-by-computer (and user-by-user) basis. This means that each time a domain user logs on to a different Windows 2000 computer, a new user profile is created for that user and stored on that computer. If a domain user routinely logs on to five different Windows 2000 computers, that user has five different user profiles, one stored on each of the five computers.

In general, then, administrators don't need to create user profiles for users because Windows 2000 automatically creates a user profile for each user of every Windows 2000 computer. Administrators can, however, manually assign a roaming or mandatory user profile to a user — I'll cover these topics a bit later in this chapter.

You may be wondering how Windows 2000 actually creates user profiles. To some extent, the process depends on whether the user is logging on by using a local user account or a domain user account:

- If no user profile exists when a *local* user logs on, Windows 2000 creates a new user profile for the user by copying the entire contents of the local `Default User` profile folder to a new folder on the local computer named after the user's account.
- If no user profile exists when a *domain* user logs on, Windows 2000 checks to see whether a domain-wide `Default User` profile folder exists in the `NETLOGON` share on the domain controller.
    - ▶ If Windows 2000 finds a domain-wide `Default User` profile folder in the `NETLOGON` share on the domain controller, it copies the entire contents of that folder to a new folder on the local computer named after the user's account.
    - ▶ If Windows 2000 doesn't find a domain-wide `Default User` profile folder in the `NETLOGON` share on the domain controller, it copies the entire contents of the *local* `Default User` profile folder to a new folder on the local computer named after the user's account.

By default, Windows 2000 stores a user's profile in the `C:\Documents and Settings\`*`user_name`* folder on the computer the user logs on to.

When Windows 2000 creates a new user profile, the new user's initial user profile is an exact copy of either the local or domain-wide `Default User` profile folder (depending on the folder Windows 2000 copied to create the new user profile).

The `Default User` profile folder can be customized by the Administrator, as I'll explain in the next section.

Customizing the Local Default User Profile Folder

Administrators can customize the local `Default User` profile folder on an individual Windows 2000 computer so that new users of this computer, at first logon, have the appropriate desktop and work environment settings. For example, you might want to place a shortcut to a network application on the desktop of all new users. Or, you might want to add a shortcut that will appear in the Start menu for all new users of this computer.

TIP

Remember that the `Default User` profile folder only affects *first-time users* of this computer—previous users already have individual user profile folders.

To customize the local `Default User` profile folder on a Windows 2000 computer, an Administrator can either copy an existing user profile to the local `Default User` profile folder, or create shortcuts in the local `Default User` profile subfolders.

The System application in Control Panel is used to copy user profiles.

TIP

You can't use Windows Explorer to copy user profiles. You can only copy user profiles by using the System application in Control Panel.

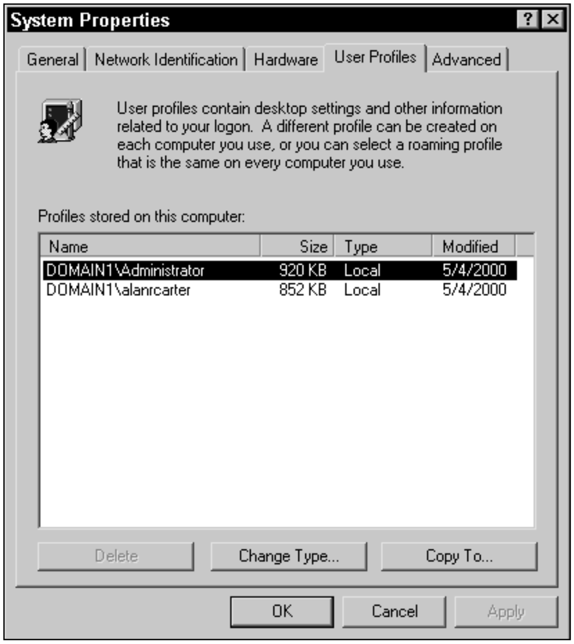
STEP BY STEP

COPYING A USER PROFILE

1. Select Start ➪ Settings ➪ Control Panel. Then double-click the System icon. (Or, from the desktop, right-click My Computer, and select Properties from the menu that appears.)
2. In the System Properties dialog box, click the User Profiles tab.
3. The User Profiles tab appears, as shown in Figure 9-15. Highlight the existing user profile that you want to copy. Click Copy To.

STEP BY STEP

Continued



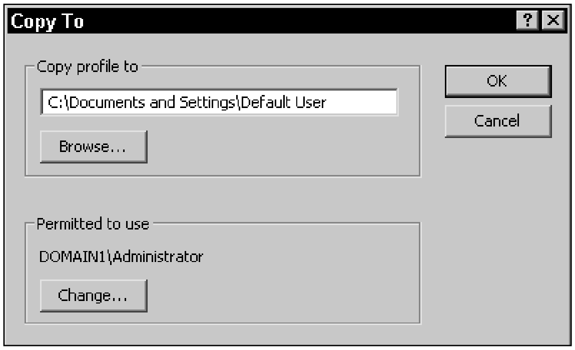
User profiles contain desktop settings and other information related to your logon. A different profile can be created on each computer you use, or you can select a roaming profile that is the same on every computer you use.

Profiles stored on this computer:

Name	Size	Type	Modified
DOMAIN1\Administrator	920 KB	Local	5/4/2000
DOMAIN1\alanrcarter	852 KB	Local	5/4/2000

FIGURE 9-15 Copying a user profile

4. In the Copy To dialog box, type the full path of the location to which you want to copy the user profile. (This could be `C:\Documents and Settings\Default User` if you are copying an existing profile to replace the current local `Default User` profile folder.) Figure 9-16 shows the Copy To dialog box after it has been configured. Notice which user is permitted to use the copied user profile.



Copy profile to

C:\Documents and Settings\Default User

Permitted to use

DOMAIN1\Administrator

FIGURE 9-16 Specifying the destination for the copied user profile

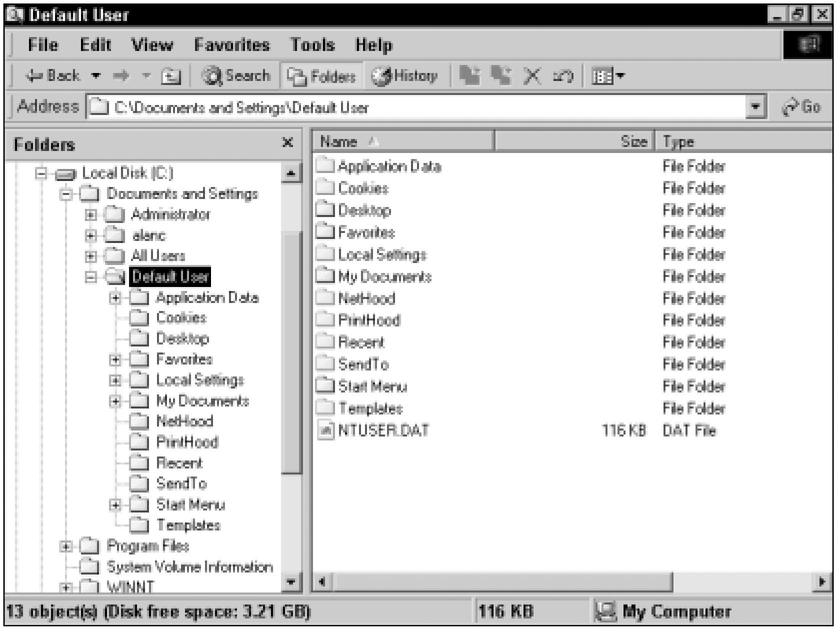
To specify the user(s) who will be permitted to use the copied user profile, click Change.

STEP BY STEP *Continued*

5. In the Select User or Group dialog box, select the user or group that you want to permit to use the copied user profile. (If you're copying a user profile to customize a `Default User` profile folder, you might want to select the Everyone group.) Click OK.
6. The Copy To dialog box reappears, with the user or group you selected in Step 5 displayed in the "Permitted to use" section of the dialog box. Click OK.
7. If the destination location you selected in Step 4 already exists (such as the location of an existing user or `Default User` profile folder) a Confirm Copy dialog box appears, notifying you that the current contents of the destination folder will be deleted during this operation. Click Yes to copy the user profile to the new location and to overwrite the existing contents.
8. In the System Properties dialog box, click OK.

CREATING SHORTCUTS IN THE DEFAULT USER PROFILE SUBFOLDERS

1. Select Start ➪ Programs ➪ Accessories ➪ Windows Explorer.
2. In the left pane, click the + next to My Computer. Click the + next to Local Disk (C:). Click the + next to Documents and Settings. Click the + next to Default User. Figure 9-17 shows the `Default User` profile folder in Windows Explorer.



Address C:\Documents and Settings\Default User

Name	Size	Type
Application Data		File Folder
Cookies		File Folder
Desktop		File Folder
Favorites		File Folder
Local Settings		File Folder
My Documents		File Folder
NetHood		File Folder
PrintHood		File Folder
Recent		File Folder
SendTo		File Folder
Start Menu		File Folder
Templates		File Folder
NTUSER.DAT	116 KB	DAT File

13 object(s) (Disk free space: 3.21 GB) 116 KB My Computer

FIGURE 9-17 The Default User profile folder

STEP BY STEP *Continued*

3. In the left pane, highlight the subfolder of the `Default User` profile folder in which you want to create a shortcut. Select File ➪ New ➪ Shortcut.
4. In the Create Shortcut dialog box, type the full path to the application. If you don't know the full path to the application, you can browse for it. Click Next.
5. In the Select a Title for the Program dialog box, type the name of the shortcut the way you want it to appear on the user's desktop. Click Finish.
6. Repeat Steps 3 through 5 until you have created all the shortcuts you want in the `Default User` profile folder. Close Windows Explorer.

Creating and Customizing a Domain-wide Default User Profile Folder

In addition to (or instead of) customizing the local `Default User` profile folder on a Windows 2000 computer, you can create a domain-wide `Default User` profile folder for all Windows 2000 computers in a domain.

While changes to the local `Default User` profile folder on a Windows 2000 computer affect only first-time users who log on to the local computer, the domain-wide `Default User` profile folder affects all domain users the first time they log on to any Windows 2000 computer in the domain.

Windows 2000 doesn't automatically create a domain-wide `Default User` profile folder — you must manually create it.

To create a domain-wide `Default User` profile folder, first customize any existing user profile or `Default User` profile folder on any Windows 2000 computer in the domain so that it has the settings and shortcuts you want the new domain-wide `Default User` profile folder to have. Then use the System application in Control Panel to copy the customized profile folder to the `NETLOGON` share on any domain controller in the domain.

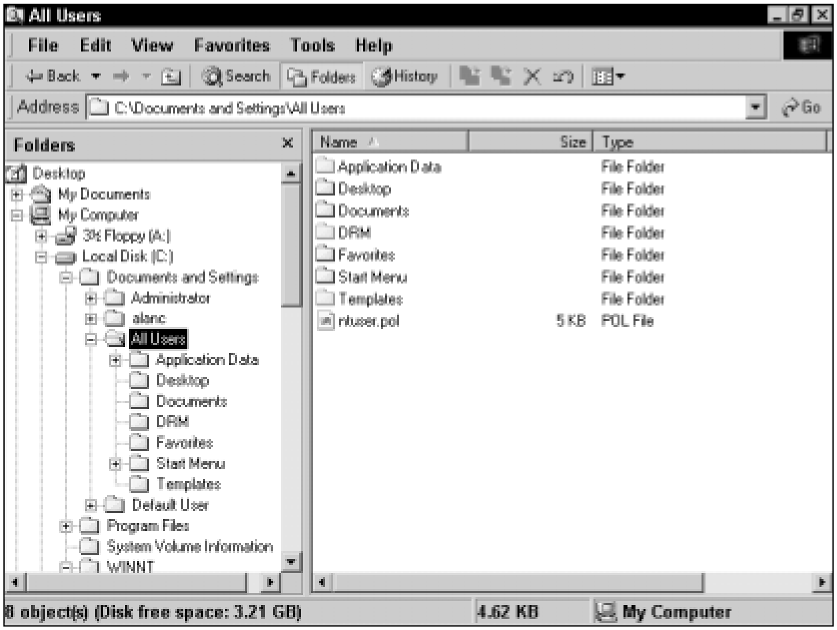
TIP

In order for the new domain-wide `Default User` profile folder to work correctly, you must name the copied folder `Default User`, and you must configure the copied folder so the Everyone group is permitted to use it.

By default, the NETLOGON share is located in the *SystemRoot*\SYSVOL\sysvol\domain_name\SCRIPTS folder on each domain controller in the domain. Because the NETLOGON share is located in a subfolder of the \SYSVOL folder, Windows 2000 will automatically replicate the domain-wide Default User profile folder to all other domain controllers in the domain.

Customizing the All Users Profile Folder

The All Users profile folder is a subfolder of the Documents and Settings folder on all Windows 2000 computers. The All Users profile folder contains seven subfolders, as shown in Figure 9-18.



Address: C:\Documents and Settings\All Users

Name	Size	Type
Application Data		File Folder
Desktop		File Folder
Documents		File Folder
DRM		File Folder
Favorites		File Folder
Start Menu		File Folder
Templates		File Folder
ntuser.pol	5 KB	POL File

8 object(s) (Disk free space: 3.21 GB) 4.62 KB My Computer

FIGURE 9-18 The All Users profile folder

The purpose of the All Users profile folder is to enable an Administrator to create shortcuts and install applications that he or she wants to make available to *all* (not just first-time) users of a Windows 2000 computer.

Whenever a user logs on to a Windows 2000 computer, any files, shortcuts, or applications placed in any of the subfolders in the All Users profile folder will appear on the user's desktop, Start menu, or other appropriate location. Only members of the Administrators group on the local computer can customize the All Users profile folder.

The `All Users` profile folder must be managed on a computer-by-computer basis. There is currently no method to create a domain-wide `All Users` profile folder on a server. This means the Administrator must customize the `All Users` profile folder on each individual Windows 2000 computer.

To customize the `All Users` profile folder, follow the same steps you would use to customize the local `Default User` profile folder, except select the `All Users` profile folder in Windows Explorer instead of the `Default User` profile folder.

Roaming User Profiles

Roaming user profiles are user profiles that are stored on a Windows 2000 Server computer. Because these profiles are stored on a server instead of on the local computer, they are available to users regardless of which Windows 2000 computer on the network they log on to.

The benefit of using roaming user profiles is that users retain their own customized desktop and work environment settings even though they may use several different Windows 2000 computers.

Roaming user profiles are implemented by first creating a shared folder on a Windows 2000 Server computer, and then assigning a server-based user profile path to a user account.

STEP BY STEP

PART 1: CREATING A SHARED FOLDER ON A SERVER

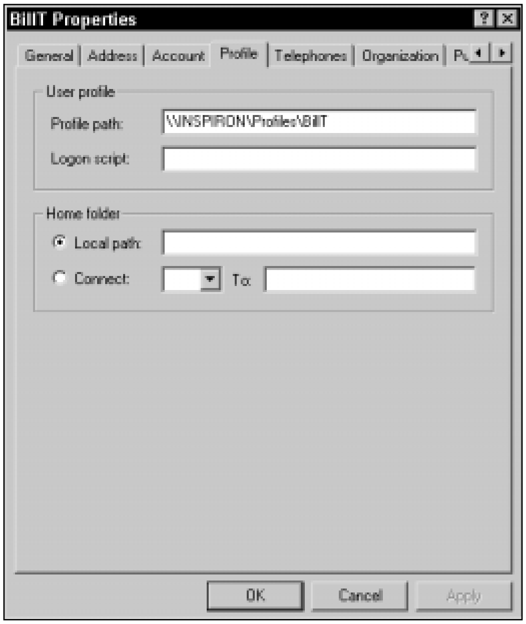
1. Choose a Windows 2000 Server computer on your network on which to store roaming user profiles. (This is often a domain controller.)
2. Create a shared folder on the server. To do this, select Start ➪ Programs ➪ Accessories ➪ Windows Explorer.
3. In the left pane, click the + next to My Computer. Highlight one of the drives on the server. (This drive must have enough free space to contain your roaming user profiles.) Select File ➪ New ➪ Folder.
4. Type in a name for the new folder and press Enter. (I recommend you use the name **Profiles**.) Right-click the newly created folder, and select Sharing from the menu that appears.
5. In the new folder's Properties dialog box, select the "Share this folder" option. Accept the default share name and click OK.
6. Close Windows Explorer.

STEP BY STEP *Continued*

At this point you've created a shared folder on the server. Now you must assign a server-based user profile path to each user you want to assign a roaming user profile. Use the steps in Part 2 to assign a server-based user profile path to a domain user account. Use the steps in Part 3 to assign a server-based user profile path to a local user account.

PART 2: ASSIGNING A SERVER-BASED USER PROFILE PATH TO A DOMAIN USER ACCOUNT

1. Start Active Directory Users and Computers. (Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.)
2. In the left pane of the Active Directory Users and Computers dialog box, click the + next to the name of the domain that contains the user account for which you want to configure a roaming user profile. Highlight the `Users` folder or the OU that contains the desired user account. In the right pane, double-click the user account. Or, you can right-click the user account, and select Properties from the menu that appears.
3. The user's Properties dialog box appears. Click the Profile tab.
4. The Profile tab appears. In the "Profile path" text box, type in the complete path to the shared folder you created in Part 1, and append the user's name to the end of this path. (For example, on a server named SERVER01, you might use the path `\\SERVER01\Profiles\BillT`.) Figure 9-19 shows the Profile tab after it has been configured with a server profile path. Click OK.



Profile path: \\INSPIRON\Profiles\BillT

● Local path:

○ Connect:

FIGURE 9-19 Assigning a server-based user profile path

STEP BY STEP *Continued*

5. Close Active Directory Users and Computers.

PART 3: ASSIGNING A SERVER-BASED USER PROFILE PATH TO A LOCAL USER ACCOUNT

1. From the desktop, right-click My Computer, and select Manage from the menu that appears.
2. In the Computer Management dialog box, click the + next to Local Users and Groups. Highlight the `Users` folder. In the right pane, double-click the user for whom you want to configure a roaming user profile. Or, you can right-click the user, and select Properties from the menu that appears.
3. The user's Properties dialog box appears. Click the Profile tab.
4. The Profile tab appears. In the "Profile path" text box, type in the complete path to the shared folder you created in Part 1, and append the user's name to the end of this path. (For example, on a server named SERVER02, you might use the path `\\SERVER02\Profiles\JulieC`.) Click OK.
5. Close the Computer Management dialog box.

At this point, all you've done is assign a location for the user's roaming user profile. Now the user must log on and log off to create a roaming user profile on the server. When the user logs off, the user's local user profile is saved to the server and then becomes the user's roaming user profile. The roaming user profile is then available to the user from any Windows 2000 computer to which the user logs on. From this point on, every time the user logs off, the user's roaming user profile will be updated with any changes the user has made during the time the user was logged on.

Both new and existing users can be assigned roaming user profiles. You can also preconfigure a new or existing user's roaming user profile so that the next time the user logs on, the properties of the preconfigured server-based roaming user profile are applied to the user. The advantage of using preconfigured roaming user profiles is that the Administrator can provide users with all of the shortcuts and program items users need to perform their day-to-day tasks.

To preconfigure a user's roaming user profile, assign a server-based profile path to a user account, and then copy an existing user profile (that you have customized with all of the files, shortcuts, settings, and applications you want the user to have) to the user's roaming user profile path, and ensure that the user is permitted to use the profile.

Mandatory User Profiles

A *mandatory user profile* is a user profile that, when assigned to a user, can't be changed by the user. A user can make changes to desktop and work environment settings during a single logon session, but these changes are *not* saved to the mandatory user profile when the user logs off. Each time the user logs on, the user's desktop and work environment settings revert to those contained in the mandatory user profile.

In most cases, an administrator permits users to change and customize their own user profiles. There are instances, however, when you might want to use mandatory user profiles:

- When "problem users" require a significant amount of administrator time
- When an administrator has a large number of users to administer

Occasionally, a "problem user" modifies his or her profile so that needed shortcuts and applications are deleted, and the administrator must fix the user's profile by reinstalling the necessary items. If this happens too frequently, the administrator might choose to assign the user a mandatory user profile.

To make an individual user's profile (either local or roaming) a mandatory user profile, rename the user's NTUSER.DAT file (in the user's profile folder) as NTUSER.MAN. The mandatory profile will become effective the next time the user logs on.

Sometimes an administrator needs to create a standardized desktop and work environment settings for a large number of users with similar job tasks. To accomplish this, the administrator can assign a single, customized mandatory roaming user profile to multiple user accounts.

TIP

If you have a need for the capabilities of mandatory user profiles, consider using group policy instead. Group policy provides the administrator with more control over users' environment settings than mandatory user profiles. I'll cover group policy in Chapter 10.

Deleting User Profiles

You should consider deleting user profiles for user accounts that have been deleted. Deleting a user profile by using the System application in Control Panel removes the entire user profile folder for the specified user, and also removes any Windows 2000 registry entries related to that user profile. Simply deleting the user profile folder by using Windows Explorer does *not* completely delete all settings related to the user profile.

STEP BY STEP

DELETING A USER PROFILE

1. Select Start ➪ Settings ➪ Control Panel. Then double-click the System icon. (Or, from the desktop, right-click My Computer, and select Properties from the menu that appears.)
2. In the System Properties dialog box, click the User Profiles tab.
3. On the User Profiles tab, highlight the user profile you want to delete. Click Delete.
4. In the Confirm Delete dialog box, click Yes to delete the user profile.
5. On the User Profiles tab, click OK.
6. Exit Control Panel if you opened it in Step 1.

Managing Account Policies

Windows 2000 account policies are sets of rules that are applied to user accounts. Account policies are not set on an individual account basis. Rather, they are set to apply to many users, often to all of the users in a domain. You must be a member of the Administrators group to manage account policies.

There are three major types of account policies:

- Password policy
- Account lockout policy
- Kerberos policy

I'll discuss each of these types of account policies in the sections that follow, and then show you how to set Windows 2000 account policies.

EXAM TIP

Windows 2000 account policies are fairly straightforward, but expect to see at least one password policy or account lockout policy question on both the Professional and Server exams.

Password Policy

Password policy dictates the requirements of user passwords and how often users must change their passwords. There are six configurable password policy settings: "Enforce password history," "Maximum password age," "Minimum password age," "Minimum password length," "Passwords must meet complexity requirements," and "Store password using reversible encryption for all users."

Enforce Password History The "Enforce password history" setting specifies how many different passwords a user must use before an old password can be reused. (In Windows NT 4.0, this setting was called Password Uniqueness.) You can configure any number from 0 to 24 for this setting. The default "Enforce password history" setting for a domain is "1 passwords remembered."

If this setting is configured to "0 passwords remembered," users can cycle back and forth between their two favorite passwords each time they are required to change their passwords.

If this setting is configured to "*x* passwords remembered," (where *x* represents a number from 1 through 24), users must use at least the number of new passwords specified before they can reuse an old password.

You can multiply the number of passwords remembered in "Enforce password history" times the number of days specified in "Minimum password age" to determine the number of days that must pass before a user can reuse an old password.

Maximum Password Age The "Maximum password age" setting determines the number of days a user may use the same password. You can configure any number from 0 to 999 days for this setting. The default "Maximum password age" setting is 42 days (six weeks).

If this setting is configured to 0 days, users are never required to change their passwords.

If this setting is configured to *x* days (where *x* represents a number from 1 through 999), Windows 2000 forces users to change their passwords when the "Maximum password age" setting is exceeded. Normal settings for "Maximum password age" are between thirty and ninety days.

TIP

If users are not forced to change their passwords often enough, network security may be compromised. However, if users have to change their passwords too frequently, they may be unable to remember their passwords.

Minimum Password Age The "Minimum password age" setting determines the number of days a user must keep the same password. You can configure any number from 0 to 998 days for this setting. The default "Minimum password age" setting is 0 days.

Windows 2000 requires that the "Minimum password age" setting be at *least* one day less than the "Maximum password age" setting, in order to permit users to change their passwords before they expire. I recommend that you set the "Minimum password age" setting at least five days less than the "Maximum password age" setting.

If this setting is configured to 0 days, users can change their passwords as often as they like, without waiting for any time to pass before selecting a new password.

If this setting is configured to *x* days (where *x* represents a number from 1 through 998), users must use their passwords for at least the number of days specified before Windows 2000 will let them change their passwords.

Password policy settings are designed to work in conjunction with each other. You can't always just configure one setting and forget the rest. For example, if you accept the default "Minimum password age" setting of 0 days, and the "Enforce password history" setting is configured to "8 passwords remembered," a user may be tempted to bypass the intent of the "Enforce password history" setting by changing his or her password nine times, in rapid succession, so the user can recycle back to the user's original, favorite, and easily remembered password.

Minimum Password Length The "Minimum password length" setting specifies the minimum number of characters required in users' passwords. You can configure any number from 0 to 14 characters for this setting. The default "Minimum password length" setting is 0 characters.

If this setting is configured to 0 characters, users are not required to have passwords.

If this setting is configured to *x* characters (where *x* represents a number from 1 through 14), you can specify the minimum number of characters a user's password must contain. Windows 2000 will not permit users to choose a password with *fewer* than the required number of characters.

TIP

I recommend a minimum of eight characters for the "Minimum password length" setting. With a password length of eight characters or more, assuming basic password security measures are taken, it's statistically almost impossible for an unauthorized user to guess a password.

Passwords Must Meet Complexity Requirements The "Passwords must meet complexity requirements" setting determines whether user passwords must contain a combination of specified characters. This setting can either be enabled or disabled. By default, the "Passwords must meet complexity requirements" setting is disabled.

When this setting is disabled, user passwords may contain any type or combination of characters.

When this setting is enabled, user passwords must contain at least one character from at least three of the following four categories:

- Lowercase alphabetic characters
- Uppercase alphabetic characters
- Numbers
- Special characters

For example, the password JB1234QR does *not* meet the password complexity requirements because it contains only uppercase alphabetic characters and numbers. However, the password JB1234qr *does* meet the complexity requirements, because it uses uppercase alphabetic characters, lowercase alphabetic characters, and numbers.

Store Password Using Reversible Encryption for All Users The "Store password using reversible encryption for all users" setting determines whether Windows 2000 stores user passwords by using one-way encryption or by using reversible encryption. One-way encryption is more secure than reversible encryption. This setting can either be enabled or disabled. By default, the "Store password using reversible encryption for all users" setting is disabled.

When this setting is disabled, Windows 2000 stores user passwords by using one-way encryption. When this setting is enabled, Windows 2000 stores user passwords by using reversible encryption.

This setting should only be enabled when most or all users in the domain log on to the Windows 2000 domain from Apple computers, because Apple computers don't support the Windows 2000 implementation of one-way encryption.

If only a few users log on to the Windows 2000 domain from Apple computers, configure the individual user accounts to "Store password using reversible encryption" instead of setting an account policy.

Account Lockout Policy

Account lockout policy dictates how Windows 2000 treats a user account after several successive unsuccessful logon attempts have occurred. There are three configurable settings: "Account lockout threshold," "Account lockout duration," and "Reset account lockout counter after."

Account Lockout Threshold

The "Account lockout threshold" setting specifies the number of successive unsuccessful logon attempts that will be permitted before Windows 2000 locks out a user account. The possible settings are from 0 to 999 invalid logon attempts. The default "Account lockout threshold" setting is 0 invalid logon attempts.

If this setting is configured to 0 invalid logon attempts, user accounts will never be locked out, regardless of the number of successive unsuccessful logon attempts.

If this setting is configured to *x* invalid logon attempts (where *x* represents a number from 1 through 999), Windows 2000 will lock out a user account after the specified number of successive unsuccessful logon attempts is reached. This setting's counter is reset to 0 after each *successful* logon. Windows 2000 maintains a separate counter for each user account.

Account Lockout Duration

The "Account lockout duration" setting specifies how long a user account is locked out after the specified number of bad logon attempts occurs. The possible settings are: "Not defined," or from 0 to 99,999 minutes. The default "Account lockout duration" setting is "Not defined."

If this setting is "Not defined," user accounts will never be locked out, and there will not be an account lockout duration.

Contrary to what it sounds like, if this setting is configured to 0 minutes, user accounts will be locked out, not for 0 minutes, but *until the Administrator unlocks the account*.

If this setting is configured to *x* minutes (where *x* represents a number from 1 through 99,999), user accounts will be locked out either until the Administrator unlocks the account, or until the number of specified minutes have passed, whichever occurs first.

Reset Account Lockout After The "Reset account lockout after" setting specifies the number of minutes that must pass without a bad logon attempt in order for the "Account lockout threshold" counter to be reset to zero. Resetting the counter to zero gives users the full number of possible bad logon attempts before account lockout. The possible settings are: "Not defined," or from 1 to 99,999 minutes. The default "Reset account lockout after" setting is "Not defined."

If this setting is "Not defined," user accounts will never be locked out, and the "Reset account lockout after" setting won't be used.

If this setting is configured to *x* minutes (where *x* represents a number from 1 through 99,999), the "Account lockout threshold" counter will be reset to zero after the specified number of minutes have passed with no bad logon attempts.

Kerberos Policy

Kerberos policy dictates how Windows 2000 uses the Kerberos V5 authentication protocol to authenticate users. There are five configurable settings:

- Enforce user logon restrictions
- Maximum lifetime for service ticket
- Maximum lifetime for user ticket
- Maximum lifetime for user ticket renewal
- Maximum tolerance for computer clock synchronization

The default configurations for each of these five settings are adequate for most Windows 2000 implementations, and should not be changed except by Administrators who have an in-depth understanding of the Kerberos V5 protocol.

Setting Account Policies

Although account policies are applied to user accounts, the policies are actually configured on individual Windows 2000 computers or groups of computers. Then the account policies are applied to users as they log on to a computer.

Account policies can be set for the local Windows 2000 computer, for all Windows 2000 computers in a domain, for all domain controllers in a domain, or for all Windows 2000 computers in a particular organizational unit (OU) in a domain. (The exception to this is Kerberos policy, which can't be configured for the local computer or for all computers in an OU.) The most common way to set account policies is to set the policies for all Windows 2000 computers in the domain.

Sometimes account policies are set in more than one place. For example, account policies may be set for the local computer and also set for the domain. When account policies conflict, the policy with the highest priority is applied. The levels of account policy priority, from greatest to least, are:

1. Account policies for an OU
2. Account policies for the domain
3. Account policies for domain controllers
4. Account policies for the local computer

The tool you use to set account policies depends on where you want to set account policies:

- To set account policies on the local Windows 2000 computer, use the Local Security Policy tool in Administrative Tools. (Select Start ➪ Settings ➪ Control Panel, double-click Administrative Tools, then double-click Local Security Policy.)
- To set account policies for all Windows 2000 computers in a domain, use the Domain Security Policy tool in Administrative Tools. (Select Start ➪ Programs ➪ Administrative Tools ➪ Domain Security Policy.) This tool is available on Windows 2000 domain controllers, or on other Windows 2000 computers that have the ADMINPAK installed.
- To set account policies for all domain controllers in a domain, use the Domain Controller Security Policy tool in Administrative Tools. (Select Start ➪ Programs ➪ Administrative Tools ➪ Domain

Controller Security Policy.) This tool is available on Windows 2000 domain controllers, or on other Windows 2000 computers that have the ADMINPAK installed.

- To set account policies for all Windows 2000 computers in a particular OU in a domain, use Active Directory Users and Computers to configure a group policy for the OU that specifies the desired account policies.

TIP

Another way to set account policies is to use Active Directory Users and Computers to configure a group policy for the domain (or for the domain controllers in the domain) that specifies the desired account policies. I'll explain how to use group policy in Chapter 10.

Now I'll show you how to set account policies for all Windows 2000 computers in the domain by using the Domain Security Policy tool. Because the Windows 2000 user interfaces for the Domain Security Policy tool, the Domain Controller Security Policy tool, and the Local Security Policy tool are substantially similar, you can use these same steps to set account policies for domain controllers or for the local Windows 2000 computer by using the appropriate tool.

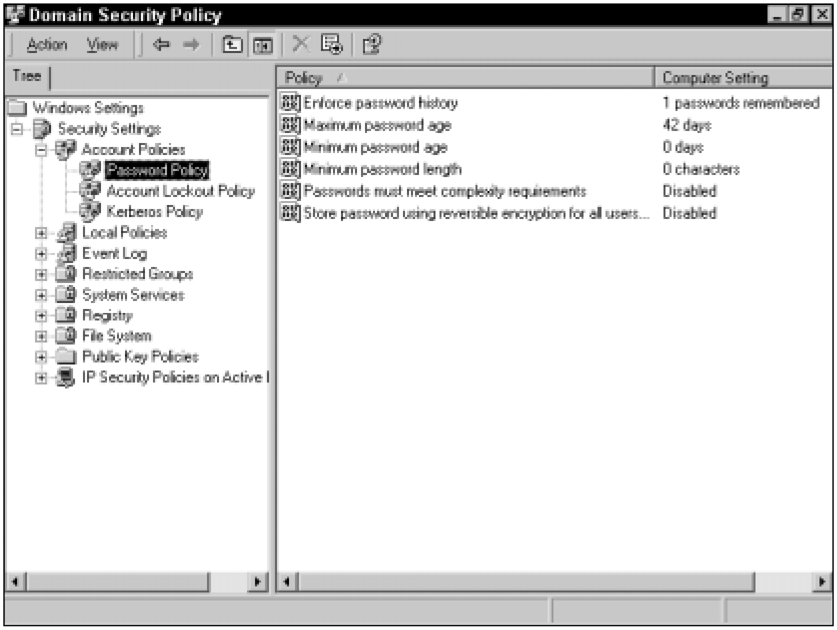
STEP BY STEP

SETTING ACCOUNT POLICIES FOR THE DOMAIN

1. Start the Domain Security Policy tool. (Select Start ➪ Programs ➪ Administrative Tools ➪ Domain Security Policy.)
2. In the left pane of the Domain Security Policy dialog box, click the + next to Security Settings. Then click the + next to Account Policies.
3. In the left pane of the dialog box, highlight the type of account policies you want to set, either Password Policy, Account Lockout Policy, or Kerberos Policy.

   Figure 9-20 shows Password Policy highlighted in the Domain Security Policy dialog box. Notice the six configurable settings displayed in the right pane.
4. To set account policies, in the right pane, double-click the setting you want to configure. For example, suppose you want to configure the minimum password length.

STEP BY STEP *Continued*

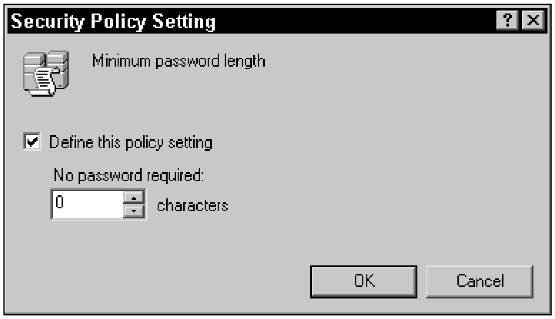


- Windows Settings
  - Security Settings
    - Account Policies
      - Password Policy
      - Account Lockout Policy
      - Kerberos Policy
    - Local Policies
    - Event Log
    - Restricted Groups
    - System Services
    - Registry
    - File System
    - Public Key Policies
    - IP Security Policies on Active I

Policy	Computer Setting
Enforce password history	1 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Passwords must meet complexity requirements	Disabled
Store password using reversible encryption for all users...	Disabled

FIGURE 9-20 Setting password policy

5. In this case, the Security Policy Setting dialog box would be displayed, as shown in Figure 9-21. Notice that a spin box is used to specify the minimum number of required characters in user passwords.



Minimum password length

☑ Define this policy setting

No password required:

0 characters

FIGURE 9-21 Setting minimum password length

TIP

Most of the Security Policy Setting dialog boxes, which are used for setting password policy, account lockout policy, and Kerberos policy, are similar to the dialog box shown in Figure 9-21.

STEP BY STEP *Continued*

Make the appropriate configurations in the Security Policy Setting dialog box and click OK.

6. Repeat Steps 3 through 5 to set additional account policies as necessary. When you've finished setting account policies, close the Domain Security Policy dialog box.

TIP

Changes made to domain security policy are made on only one domain controller. It may take several minutes to several hours for these changes to replicate to all domain controllers in the domain. During this time, some users will experience the changes, and some won't.

Managing User Rights

User rights authorize users and groups to perform specific tasks on a Windows 2000 computer or in a Windows 2000 domain. User rights are *not* the same as permissions: user rights enable users to perform tasks; whereas permissions enable users to access objects, such as files, folders, printers, and Active Directory objects. You must be a member of the Administrators group to assign user rights.

In the following sections I'll discuss specific Windows 2000 user rights, and also explain how to assign user rights.

User Rights

Each user right authorizes a user or group to perform a specific task. User rights, unlike account policies, can be assigned to individual users and groups.

Microsoft has subdivided Windows 2000 user rights into two categories: logon rights and privileges. *Logon rights* specify whether a user is permitted to authenticate (log on) to a Windows 2000 computer, and if so, how that user is permitted to log on. *Privileges* enable a user to perform specific tasks.

The Windows 2000 logon rights are:

- Access this computer from the network
- Deny access to this computer from the network
- Deny logon as a batch job
- Deny logon as a service

- Deny logon locally
- Log on as a batch job
- Log on as a service
- Log on locally

TIP

When a user is assigned both the "Log on locally" and the "Deny logon locally" logon rights or when logon rights conflict, the "Deny logon locally" logon right takes precedence.

The Windows 2000 privileges are:

- Act as part of the operating system
- Add workstations to domain
- Back up files and directories
- Bypass traverse checking
- Change the system time
- Create a pagefile
- Create a token object
- Create permanent shared objects
- Debug programs
- Enable computer and user accounts to be trusted for delegation
- Force shutdown from a remote system
- Generate security audits
- Increase quotas
- Increase scheduling priority
- Load and unload device drivers
- Lock pages in memory
- Manage auditing and security log
- Modify firmware environment values
- Profile single process
- Profile system performance
- Remove computer from docking station
- Replace a process level token

- Restore files and directories
- Shut down the system
- Synchronize directory service data
- Take ownership of files or other objects

Most of these user rights are self explanatory. For detailed descriptions of any of these logon rights or privileges, view the Windows 2000 Help topics (on a Windows 2000 Server computer) titled “Logon rights” and “Privileges.”

Assigning User Rights

Although user rights are applied to user and group accounts, user rights are actually configured for individual Windows 2000 computers or groups of computers.

User rights can be set for the local Windows 2000 computer, for all Windows 2000 computers in a domain, for all domain controllers in a domain, or for all Windows 2000 computers in a particular OU in a domain. The most common way to assign user rights is to configure them for all Windows 2000 computers in the domain.

You can assign user rights in much the same way that you set account policies. The tool you use to assign user rights depends on where you want to configure them:

- To assign user rights for the local Windows 2000 computer, use the Local Security Policy tool in Administrative Tools. (Select Start ➪ Settings ➪ Control Panel, double-click Administrative Tools, then double-click Local Security Policy.)
- To assign user rights for all Windows 2000 computers in a domain, use the Domain Security Policy tool in Administrative Tools. (Select Start ➪ Programs ➪ Administrative Tools ➪ Domain Security Policy.) This tool is available on Windows 2000 domain controllers, or on other Windows 2000 computers that have the ADMINPAK installed.
- To assign user rights for all domain controllers in a domain, use the Domain Controller Security Policy tool in Administrative Tools. (Select Start ➪ Programs ➪ Administrative Tools ➪ Domain Controller Security Policy.) This tool is available on Windows 2000 domain controllers, or on other Windows 2000 computers that have the ADMINPAK installed.

- To assign user rights for all Windows 2000 computers in a particular OU in a domain, use Active Directory Users and Computers to configure a group policy for the OU that specifies the desired account policies.

TIP

Another way to assign user rights is to use Active Directory Users and Computers to configure a group policy for the domain (or for the domain controllers in the domain) that specifies the desired user rights. I'll explain how to use group policy in Chapter 10.

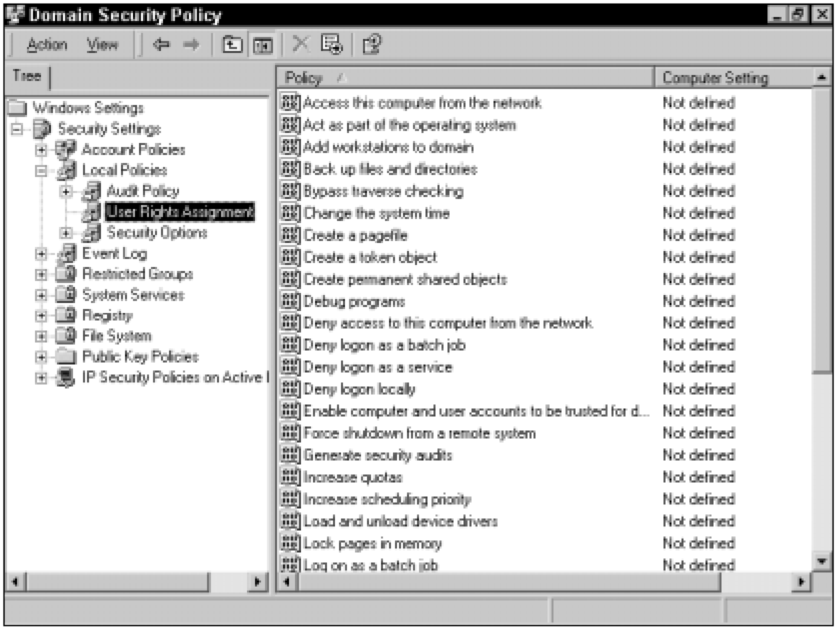
Now I'll show you how to assign user rights for all Windows 2000 computers in the domain by using the Domain Security Policy tool. Because the Windows 2000 user interfaces for the Domain Security Policy tool, the Domain Controller Security Policy tool, and the Local Security Policy tool are very similar, you can use these same steps to configure user rights for domain controllers or for the local Windows 2000 computer by using the appropriate tool.

STEP BY STEP

ASSIGNING USER RIGHTS FOR THE DOMAIN

1. Start the Domain Security Policy tool. (Select Start ➪ Programs ➪ Administrative Tools ➪ Domain Security Policy.)
2. In the left pane of the Domain Security Policy dialog box, click the + next to Security Settings. Then click the + next to Local Policies. In the left pane of the dialog box, highlight User Rights Assignment. The list of user rights that you can assign appears in the right pane, as shown in Figure 9-22. Notice that both logon rights and privileges are listed.
3. To assign user rights, in the right pane, double-click the user right you want to assign.
4. A Security Policy Setting dialog box for the user right you selected appears, as shown in Figure 9-23. Notice that the user right I chose to configure is called "Log on locally." This user right permits users to log on interactively at all Windows 2000 computers within the tool's scope, in this case, at all Windows 2000 computers in the domain.

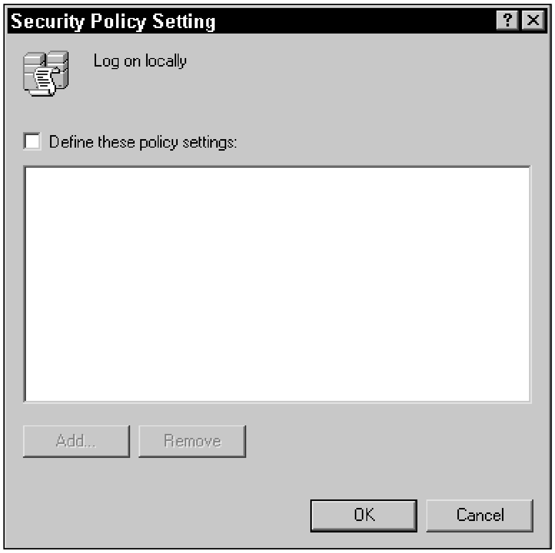
STEP BY STEP *Continued*



- Windows Settings
  - Security Settings
    - Account Policies
    - Local Policies
      - Audit Policy
      - User Rights Assignment
      - Security Options
    - Event Log
    - Restricted Groups
    - System Services
    - Registry
    - File System
    - Public Key Policies
    - IP Security Policies on Active I

Policy	Computer Setting
Access this computer from the network	Not defined
Act as part of the operating system	Not defined
Add workstations to domain	Not defined
Back up files and directories	Not defined
Bypass traverse checking	Not defined
Change the system time	Not defined
Create a pagefile	Not defined
Create a token object	Not defined
Create permanent shared objects	Not defined
Debug programs	Not defined
Deny access to this computer from the network	Not defined
Deny logon as a batch job	Not defined
Deny logon as a service	Not defined
Deny logon locally	Not defined
Enable computer and user accounts to be trusted for d...	Not defined
Force shutdown from a remote system	Not defined
Generate security audits	Not defined
Increase quotas	Not defined
Increase scheduling priority	Not defined
Load and unload device drivers	Not defined
Lock pages in memory	Not defined
Log on as a batch job	Not defined

FIGURE 9-22 Assigning user rights



Log on locally

□ Define these policy settings:

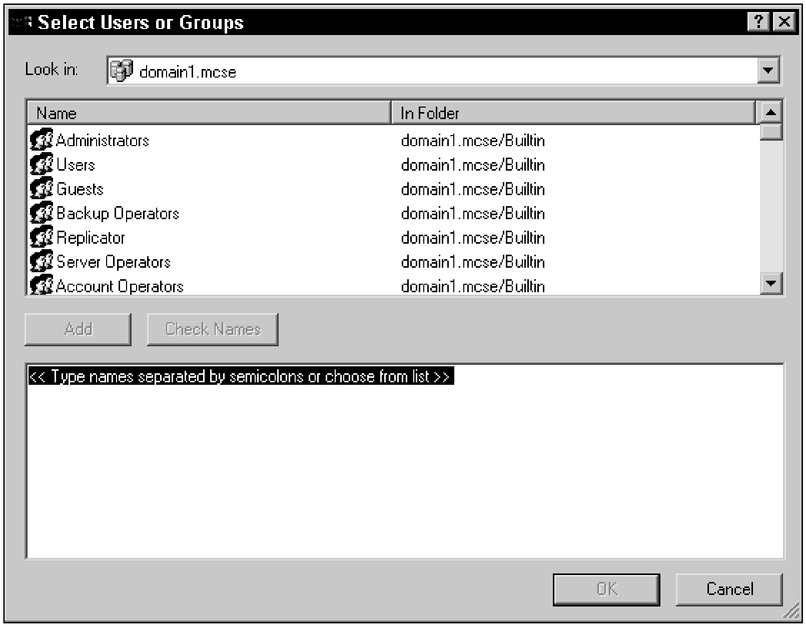
FIGURE 9-23 Assigning the "Log on locally" user right

STEP BY STEP *Continued*

If you're using the Domain Security Policy tool or Domain Controller Security Policy tool, select the check box next to "Define these policy settings" (if it is not already selected). Then click Add.

If you're using the Local Security Policy tool, click Add.

5. The "Add user or group" dialog box appears. Click Browse to add users or groups.
6. The Select Users or Groups dialog box appears, as shown in Figure 9-24.



Select Users or Groups

Look in: domain1.mcse

Name	In Folder
Administrators	domain1.mcse/Builtin
Users	domain1.mcse/Builtin
Guests	domain1.mcse/Builtin
Backup Operators	domain1.mcse/Builtin
Replicator	domain1.mcse/Builtin
Server Operators	domain1.mcse/Builtin
Account Operators	domain1.mcse/Builtin

<< Type names separated by semicolons or choose from list >>

FIGURE 9-24 Selecting users and groups

Double-click each user or group that you want to assign this user right to. As you double-click each user or group, the user or group's name will appear in the bottom section of this dialog box. (You can also perform this step by highlighting a user or group and then clicking Add, but double-clicking is faster and easier.) When you've selected all of the users and/or groups you want to assign this user right to, click OK.

7. In the "Add user or group" dialog box, click OK.
8. In the Security Policy Setting dialog box, click OK.
9. Repeat Steps 3 through 8 to assign additional user rights if necessary. When you've finished assigning user rights, close the Domain Security Policy dialog box.

Removing User Rights

The steps in the previous section explain how to *assign* user rights to a user or group, but you can also use these steps (with a few modifications) to *remove* a user right from a user or group. If you're using the Domain Security Policy tool or the Domain Controller Security Policy tool, in Step 4, instead of clicking Add, highlight the existing user or group you want to remove the user right from and click Remove. If you're using the Local Security Policy tool, in Step 4, instead of clicking Add, clear the check box next to the user or group you want to remove the user right from.

Troubleshooting User Accounts, User Rights, Account Policies, and Authentication

There are several common problems that may arise when working with user accounts. These problems generally take the form of a user not being able to log on, or not being able to access a resource or perform a task that the user needs to access or perform. The solutions to these problems frequently involve reconfiguring a user account setting, reconfiguring a user rights assignment, or changing account policies.

The following tables address common user account problems and provide some troubleshooting tips that may help you resolve these problems. Table 9-3 deals with user account settings problems. Table 9-4 addresses user rights problems. Table 9-5 explores some common account policy problems. Finally, Table 9-6 covers common user authentication problems.

TABLE 9-3 Troubleshooting User Account Settings

Problem	Troubleshooting Tips
You are an Administrator, but you are unable to modify the properties of a user account.	Verify that you are logged on as Administrator. If you are logged on as Administrator, ensure that you have the appropriate permissions to manage the user account. Verify your permissions on the Security tab in the user's Properties dialog box. If necessary, take ownership of the user account.

Continued▶

TABLE 9-3 *(continued)*

Problem	Troubleshooting Tips
A user reports that she can't log on to her Windows 2000 computer. During the logon attempt, a message stating "Your account has been disabled. Please see your system administrator" is displayed.	This message is displayed when a user's account has expired, has been disabled, or has been locked out. If the user is a local user, on the General tab in the local user's Properties dialog box, clear the check box next to "Account is locked out" or clear the check box next to "Account is disabled." If the user is a domain user, on the Account tab in the user's Properties dialog box, change the account expiration date or clear the check box next to "Account is locked out."
A user who normally works weekdays came in to work on Sunday, and could not log on to his Windows 2000 computer. A message stating "Unable to log you on because of an account restriction" was displayed.	This message is displayed when a user attempts to log on during restricted hours or attempts to log on to a restricted computer. Check the Logon Hours and Log On To settings on the Account tab in the user's Properties dialog box, and make any necessary changes.

TABLE 9-4 Troubleshooting User Rights

Problem	Troubleshooting Tips
A user reports that she is unable to log on locally to the domain controller.	By default, only Administrators can log on locally to the domain controller. Restricting local logon to the domain controller is generally a preferred practice. Use the Domain Controller Security Policy tool to grant the user the "Log on locally" user right, or make the user a member of a group that has that user right. Remember, if the user has been assigned both the "Log on locally" and "Deny logon locally" user rights, the "Deny logon locally" right takes precedence.
A user reports that he is unable to clear or save the Event Viewer logs on his Windows 2000 computer.	Use the Local Security Policy tool on the local computer to grant the user the "Manage auditing and security log" user right, or make the user a member of a group that has that user right.

TABLE 9-5 Troubleshooting Account Policies

Problem	Troubleshooting Tips
When Windows 2000 prompts a user to change his password, he types in a new password, but Windows 2000 will not accept the user's new password. A message stating "Your password must be at least 8 characters; cannot repeat any of your previous 2 passwords; must contain capitals, numerals or punctuation . . ." is displayed.	Examine the Password Policy settings. Check to see if the new password the user has entered meets the minimum password length and password complexity requirements. Remember, if password complexity is enabled, the password must contain three of the four types of characters: uppercase alphabetic, lowercase alphabetic, numbers, and special characters. Is the user's new password a password that he has used previously? If so, check to see if it meets the "Enforce password history" settings.
A user reports that she can't change her password. When she attempts to do so, a message stating "The password on this account cannot be changed at this time" is displayed.	The most likely cause of this problem is that the user hasn't met the minimum password age requirements. Explain to the user that she must keep her password for the minimum number of days specified.
Numerous users report that if they mistype their passwords two times they are unable to log on. A message stating, "Your account has been disabled. Please see your system administrator" is displayed.	Examine the Account Lockout Policy settings. The most likely cause of this problem is that the "Account lockout threshold" setting is set too low. Increase this setting if necessary. In addition, you will need to manually unlock each user's account (in the user's Properties dialog box) before they will be able to log on.

TABLE 9-6 Troubleshooting Local User Authentication

Problem	Troubleshooting Tips
A user reports that he is unable to log on. A message is displayed, stating "The system could not log you on."	Verify that the user name, domain, and password the user is using are correct. Remember, passwords are case sensitive. Make sure that Caps Lock is not on.
A user reports that she is able to log on locally (by using her local user account) but is *unable* to log on to the domain (by using her domain user account).	Verify that at least one domain controller is available on the network. If so, check the network connection between the user's computer and the domain controller.
A user at a Windows NT 4.0 computer reports that he is nable to log on to the domain.	The most likely cause of this problem is that the Windows 2000 domain controller that is performing the PDC emulator role is unavailable. Take the necessary actions to make this computer available on the network.

Creating and Managing Group Accounts

Groups are collections of user accounts. Using groups is a convenient and efficient way to assign user rights and permissions to multiple users.

There are two fundamental types of groups in Windows 2000: security groups and distribution groups. *Security groups* are primarily used to assign permissions and user rights to multiple users. In addition, security groups can be used by some e-mail programs to send messages to the list of users who are members of the group.

Distribution groups are primarily used to send e-mail messages to a specified list of users. You can't assign permissions and user rights to distribution groups. Distribution groups are an important feature because some e-mail programs are unable to send e-mail to the list of users who are members of a security group. Lastly, distribution groups can't be created on the local computer — they can only be created in Active Directory.

When I discuss groups in the rest of this chapter, I'll be talking about security groups, because only security groups can be used to assign user rights and permissions to multiple users.

Groups can be created either on the local computer or in Active Directory. In the following sections I'll discuss the various Windows 2000 groups, explain how to create groups, and show you how to configure and manage group properties.

Groups on the Local Computer

Groups on the local computer are primarily used to control access to resources on that computer. All groups on the local computer are security groups. There are two kinds of groups found on the local computer: local groups and built-in groups.

Local Groups

Local groups are groups that are created and maintained on an individual Windows 2000 computer (that is not a domain controller). Local groups can be created by members of the Administrators, Power Users, and Users groups.

Local groups are used to control access to resources on the local computer. In a typical configuration, a local group is assigned permissions to a specific resource, such as a shared folder or a shared printer. Then individual user accounts and groups are made members of this local group. The result is that all members of the local group now have permissions to the shared resource on the local computer. Using local groups simplifies the administration of resources, because permissions can be assigned once to a local group, instead of separately to each user account.

TIP

Local groups *can't* be used to control access to resources on any computer other than the local computer.

Both local and domain user accounts can be members of a local group. In addition, built-in system groups on the local computer and global groups and universal groups from the domain can be members of a local group. Finally, a local group can't be a member of another group.

Built-in Groups

Built-in groups are groups with preset characteristics that are automatically created during the installation of Windows 2000. There are two kinds of built-in groups on a Windows 2000 computer that is not a domain controller: built-in local groups, and built-in special groups.

Built-in Local Groups *Built-in local groups* are groups that have the rights and/or permissions that enable their members to perform specific tasks on the local computer. You can assign users to the built-in local groups that most closely match the tasks the users need to perform. If there isn't a built-in local group that has the rights or permissions needed to perform a specific task or access a specific resource, then you can create a local group and assign it the necessary rights or permissions to accomplish the task or access the resource.

You can assign rights and permissions to built-in local groups. In addition, you can make users members of (and remove users from) built-in local groups. (An exception is that you can't remove Administrator from the Administrators group.) Built-in local groups can be renamed, but they can't be deleted.

There are six built-in local groups that are automatically created during the installation of Windows 2000 on a nondomain controller:

- **Administrators:** Members of this group have full administrative rights and permissions to administer the local computer. This group initially contains the Administrator account, and, if the computer is a member of a domain, it contains that domain's Domain Admins global group.

- **Backup Operators:** Members of this group have permissions to back up and restore all files on the local computer, even if the user does not have permissions to all files. This group initially has no members.
- **Guests:** Members of this group can log on locally. Initially this group has no permissions to resources. This group initially contains the Guest account, which is disabled by default.
- **Power Users:** Members of this group can run applications, use local printers, and create local user and group accounts (and modify the users and groups they create). Members of this group can add users to and remove users from the Guests, Power Users, and Users groups. Members of this group can also share folders and printers. This group initially has no members.
- **Replicator:** This group, which supports directory replication processes, is included in Windows 2000 to provide backward compatibility with the Windows NT 4.0 Directory Replicator service. This group initially has no members.
- **Users:** Members of this group can run applications, create local groups (and manage the groups they create), and use local printers. This group initially contains the Authenticated Users and Interactive special groups, and, if the computer is a member of a domain, it contains that domain's Domain Users group. As new local user accounts are created, they are automatically made members of the built-in Users group.

Built-in Special Groups *Built-in special groups* are groups created by Windows 2000 that are used for specific purposes by the operating system. Special groups are sometimes called *system groups*.

You can assign user rights and permissions to special groups, and you can remove user rights and permissions from special groups. You can't assign users or groups to special groups. However, you can make a special group a member of a local group. You can't rename or delete special groups.

Membership in a special group is temporary, and is based solely on whether a specific set of membership requirements are met. A user is a member of a special group only for the time period in which the user meets the special group's membership requirements.

There are 12 built-in special groups on Windows 2000 computers that are not domain controllers:

- **Everyone:** Any user who accesses a Windows 2000 computer, either interactively or over-the-network, is considered a member of the Everyone special group. This includes all users accessing the computer using authorized user accounts, as well as users who are authenticated using an anonymous logon, such as a user who accesses a Web server over the network. If your network is connected to the Internet, over-the-network also means over the Internet. Because of this, Everyone means *everyone*. You should consider limiting the permissions assigned to the Everyone group.
- **Anonymous Logon:** Any user who accesses a Windows 2000 computer over-the-network (or over the Internet) by using an anonymous logon is considered a member of the Anonymous Logon special group.
- **Authenticated Users:** Any user who accesses a Windows 2000 computer, either interactively or over-the-network, by using an authorized user account is considered a member of the Authenticated Users special group.
- **Batch:** When a scheduled program or batch job logs on using a user account that has the "Log on as a batch job" user right, that user account is a member of the Batch special group.
- **Creator Owner:** A user who creates a file, folder, or print job is considered a member of the Creator Owner special group for that file, folder, or print job. The Creator Owner special group is used to assign permissions to creators of these objects. For example, by default the Creator Owner special group is assigned the Manage Documents permission to a printer when it is first created, so that creators of print jobs sent to this printer are able to manage their own print jobs.
- **Creator Group:** When a user of an Apple computer (or a user of a POSIX-compliant application) creates a file or folder, that user's primary group is considered a member of the Creator Group special group for that file or folder. The Creator Group special group is used to define the group ownership of the newly created file or folder.

- **Dialup:** Any user who accesses a Windows 2000 computer via a phone line, a Virtual Private Network (VPN), or a direct cable connection by using an authorized user account is considered a member of the Dialup special group.
- **Interactive:** Any user who physically sits at a computer and logs on locally to that Windows 2000 computer is a member of the Interactive special group. If you want to grant access to a resource on the local computer to users who log on locally to this computer, consider assigning the appropriate permissions to the Interactive group.
- **Network:** Any user who accesses resources on a Windows 2000 computer over-the-network is a member of the Network special group. If you want to grant access to a resource on the local computer to users who access this computer over-the-network, consider assigning the appropriate permissions to the Network group.
- **Service:** When a service logs on using a user account, that user account is a member of the Service special group.
- **System:** This special group is used by the Windows 2000 operating system. The System special group is not normally assigned any permissions to network resources.
- **Terminal Server User:** Any user who logs on to a Terminal Services session is a member of the Terminal Server User special group.

Creating and Managing Groups on the Local Computer

You can create and manage local groups by using the Local Users and Groups tool in Computer Management. You must be a member of the Administrators, Power Users, or Users groups to create a local group.

The degree to which a user can manage groups is typically determined by that user's group membership:

- A member of the Administrators group can manage all groups on the local computer.
- A member of the Power Users group can manage the Power Users, Guests, and Users groups on the local computer, as well as any local groups that the member creates.
- A member of the Users group can only manage the local groups that the member creates.

STEP BY STEP

CREATING A LOCAL GROUP ON THE LOCAL COMPUTER

1. Right-click My Computer, and select Manage from the menu that appears.
2. In the left pane of the Computer Management dialog box, click the + next to Local Users and Groups. Highlight the `Groups` folder. Select Action ➪ New Group.
3. In the New Group dialog box, type in a name for the new group in the "Group name" text box. Enter a description if you want to. Click Add to add members to this group.
4. In the Select Users or Groups dialog box, double-click each user or group you want to make a member of your new group. As you double-click each user or group, the user or group's name will appear in the bottom section of this dialog box. (You can also perform this step by highlighting a user or group and then clicking Add, but double-clicking is faster and easier.) When you've selected all of the users or groups you want to make members of this group, click OK.
5. In the New Group dialog box, click Create.
6. Repeat Steps 3 through 5 if you want to create additional local groups. Click Close.

Three of the most common local group management tasks are renaming a group, deleting a group, and changing the group's membership.

STEP BY STEP

RENAMING OR DELETING A LOCAL GROUP

1. Right-click My Computer, and select Manage from the menu that appears.
2. In the left pane of the Computer Management dialog box, click the + next to Local Users and Groups. Highlight the `Groups` folder. In the right pane, right-click the group you want to rename or delete.

   To *rename* a group, select Rename from the menu that appears, type in a new name for the group, and press Enter.

   To *delete* a group, select Delete from the menu that appears. Click Yes when Windows 2000 asks if you're sure you want to delete the group.

TIP

Remember, you can't delete the built-in local groups.

STEP BY STEP *Continued*

ADDING MEMBERS TO AND REMOVING MEMBERS FROM A LOCAL GROUP

1. Right-click My Computer, and select Manage from the menu that appears.
2. In the left pane of the Computer Management dialog box, click the + next to Local Users and Groups. Highlight the `Groups` folder. In the right pane, double-click the group you want to change the membership of.
3. The group's Properties dialog box appears.

   To *remove* a member from the group, highlight the member in the Members box, and click Remove. Skip to Step 5.

   To *add* a member to the group, click Add.
4. In the Select Users or Groups dialog box, double-click each user or group you want to add to the group. When you've selected all of the users and/or groups you want to add, click OK.
5. In the group's Properties dialog box, click OK.

On a Windows 2000 Professional computer, you can also use the Users and Passwords Control Panel application to add and remove existing local user accounts to and from existing local groups.

Groups in Active Directory

Groups in Active Directory are used to control access to network resources and to organize users who perform similar job tasks or have similar network access requirements.

There are three administrator-created kinds of groups in Active Directory: domain local groups, global groups, and universal groups. When you select one of these kinds of groups, the Windows 2000 user interface calls this selecting the *Group scope*. In addition to these three kinds of groups, there are built-in local, global, universal, and special groups in Active Directory.

Administrator-created groups in Active Directory can be either security groups or distribution groups. All of the built-in groups in Active Directory are security groups.

In the following sections I'll discuss each of the various groups in Active Directory, and then explain how to create and manage these groups.

Domain Local Groups

Domain local groups are groups that are created and maintained in Active Directory on Windows 2000 domain controllers. Domain local groups are used to control access to resources located on any computer in a Windows 2000 domain.

In a typical configuration, a domain local group is assigned permissions to a specific resource, such as a shared folder or a shared printer. Then individual user accounts and groups are made members of this domain local group. The result is that all members of the domain local group now have permissions to the shared resource.

A domain local group can contain user accounts from its domain, and from other domains in the forest. A domain local group can contain other domain local groups from its own domain, and can also contain global and universal groups from any domain in the forest.

Global Groups

Global groups, like domain local groups, are created and maintained in Active Directory on Windows 2000 domain controllers. Global groups, however, are primarily used to organize users who perform similar tasks or have similar network access requirements.

In a typical configuration, user accounts of domain users who have similar job functions are placed in a global group. Then this global group is made a member of one or more domain local groups in any domain in the forest. Each of these domain local groups is assigned permissions to a specific shared resource. The result is that members of the global group now have permissions to the shared resource(s).

Here's an example of how global groups can be used in real life. Suppose that when the company's network was first installed, the administrator created user accounts, and placed these user accounts in various global groups depending on the users' job functions. Now, the network administrator wants to assign several users permissions to a shared printer on a Windows 2000 computer. The administrator creates a new domain local group and assigns this group permissions to the shared printer. Then the administrator selects the global groups that contain the user accounts that need access to this shared printer, and makes the global groups members of the new domain local group. The result is that all domain user accounts that are members of the selected global groups now have access to the shared printer. If access to all resources is managed in this way, when a new user is created, the administrator need only make the user a member of the appropriate global group(s) in order for the user to have access to all network resources required to do his or her job.

The advantage of using global groups, then, is ease of administration—the network administrator can manage large numbers of users by placing them in a small number of global groups.

A global group can only contain user accounts and other global groups from its domain. Global groups can't contain domain local groups or universal groups from its domain, and can't contain user accounts or groups from any other domain.

Although it is not a preferred practice, you can assign user rights and permissions to global groups. Global groups can be assigned permissions to shared resources on any computer in the forest.

Universal Groups

Universal groups, like domain local groups and global groups, are created and maintained in Active Directory on Windows 2000 domain controllers. Universal groups, however, are used to organize users from *multiple domains* that perform similar job tasks or have similar network access requirements, and/or to control access to shared resources in *multiple domains*.

There's no one typical universal group configuration. For example, you can use a universal group as a "super" global group by placing users from multiple domains into the universal group, and then making the universal group a member of one or more domain local groups to which you have assigned permissions to shared resources. Or, you can use a universal group in much the same way as you'd use a domain local group, except that you can assign a universal group permission to a shared resource on any computer in the forest. In short, you can use universal groups just about any way you want to.

Universal groups provide significant advantages, but sometimes present significant challenges, too. The primary advantage of using universal groups is their open membership: user accounts, global groups, and universal groups from any domain in the forest can be members of a universal group. An additional advantage of using universal groups is that universal groups can be assigned permissions to shared resources on any computer in the forest.

The main disadvantage of using universal groups is that they can cause potential network traffic problems. Here's how this can happen. When you first create a universal group, all of the group's members are listed in the global catalog. Then, each time you change the membership of a universal group, the global catalog is updated, and this change is replicated to all global catalog servers on your network. If you have a large number of universal groups and change them frequently, this can cause significant amounts of replication traffic on your network.

Another challenge presented by universal groups is that they are *not* available if your Windows 2000 domain is operating in mixed-mode, that is, when you have both Windows 2000 domain controllers and Windows NT 4.0 backup domain controllers in your domain. Universal groups can only be used when your Windows 2000 domain is operating in native-mode.

Because of these challenges, you should only use universal groups when you need to organize users from multiple domains that perform similar job tasks or have similar network access requirements, or when you need to use a single group to control access to shared resources in multiple domains.

Built-in Groups on Domain Controllers

Built-in groups (in Active Directory) are security groups with preset characteristics that are automatically created during the installation of Active Directory. There are four kinds of built-in groups on Windows 2000 domain controllers: built-in local groups, built-in global groups, built-in universal groups, and built-in special groups.

Built-in Local Groups

Built-in local groups on domain controllers are groups that are automatically created during the installation of Active Directory and stored in the `Builtin` folder. Built-in local groups have rights and/or permissions that enable their members to perform specific tasks in Active Directory and/or on Windows 2000 domain controllers in the domain.

You can assign rights and permissions to built-in local groups on domain controllers only for resources located in Active Directory and/or on domain controllers in the domain. You can also add members to and remove members from built-in local groups on domain controllers (except that you can't remove the Administrator account from the Administrators group).

Built-in local groups on domain controllers can contain user accounts from the domain and from other domains in the forest. In addition, built-in local groups on domain controllers can contain domain local groups from the domain, and global and universal groups from any domain in the forest.

Built-in local groups on domain controllers can't contain other built-it local groups. And, built-in local groups on domain controllers can't be members of any other groups.

There are nine built-in local groups that are automatically created during the installation of Active Directory on a Windows 2000 domain controller:

- **Account Operators:** Members of this group can create, delete, and modify domain user and group accounts in the domain, except that Account Operators can't modify the Administrator account and can't modify or change the membership of the Administrators, Account Operators, Backup Operators, Print Operators, or Server Operators groups. This group initially has no members.
- **Administrators:** Members of this group have full administrative rights and permissions to administer Active Directory (including all of its domain users, groups, and other objects) and all domain controllers in the domain. This group initially contains the Administrator account, the Domain Admins group, and the Enterprise Admins group.
- **Backup Operators:** Members of this group have permissions to back up and restore all files on all domain controllers in the domain, even if the user does not have permissions to all files. This group initially has no members.
- **Guests:** Members of this group have no initial rights or permissions. This group initially contains the Domain Guests group and the Guest account.
- **Pre-Windows 2000 Compatible Access:** Members of this group have the Read permission for all domain users and groups in the domain. This group initially has no members. The purpose of this group is to enable users of Windows NT 4.0 computers to log on to the domain. If you have Windows NT 4.0 computers in the domain, you should make the Everyone group a member of this group.
- **Print Operators:** Members of this group can create and manage printers on any domain controller in the domain. This group initially has no members.
- **Replicator:** This group, which supports directory replication processes, is included in Windows 2000 to provide backward compatibility with the Windows NT 4.0 Directory Replicator service. This group initially has no members.

- **Server Operators:** Members of this group have permissions to back up and restore files and folders on all domain controllers in the domain, and can share folders on any domain controller in the domain. This group initially has no members.
- **Users:** Members of this group have no initial rights or permissions. You can assign to this group rights and permissions that you want all domain users to have. This group initially contains the Authenticated Users, Domain Users, and Interactive groups. As new domain user accounts are created, they are automatically made members of the Domain Users group, which is a member of the built-in Users group.

Built-in Global and Universal Groups Built-in global and universal groups on domain controllers are automatically created during the installation of Active Directory and stored in the `Users` folder. Built-in global and universal groups are primarily used to group users by the types of administrative tasks they can perform in Active Directory and on all computers in the Windows 2000 domain.

Built-in global and universal groups on domain controllers have the same characteristics as administrator-created global and universal groups (which were covered earlier in this chapter).

There are numerous built-in global and universal groups. Below I've listed and described the most common ones:

- **Domain Admins:** Members of this global group have no initial rights or permissions. This group initially derives all of its rights and permissions from its membership in other groups. By default, this group is a member of the domain's built-in local Administrators group and the local built-in Administrators group on all computers that are members of the domain. As a result of this group's membership in other groups, members of Domain Admins can administer Active Directory and all computers in the domain. This group initially contains the Administrator account.
- **Domain Users:** Members of this global group have no initial rights or permissions. This group initially derives all of its rights and permissions from its membership in other groups. By default, this group is a member of the domain's built-in local Users group and the local built-in Users group on all computers that are members of the domain. This group initially contains all domain user accounts

created when Active Directory is installed, including the Administrator and Guest accounts. As new domain user accounts are created, they are automatically made members of Domain Users.

- **Domain Guests:** Members of this global group have no initial rights or permissions. This group initially derives all of its rights and permissions from its membership in the domain's built-in local Guests group. This group initially contains the Guest account.
- **Enterprise Admins:** Members of this universal group have no initial rights or permissions. This group initially derives all of its rights and permissions from its membership in the domain's built-in local Administrators group in each domain in the forest. As a result of this membership, members of Enterprise Admins can administer Active Directory throughout the forest and all domain controllers in the forest. If you have multiple domains in your forest, Windows 2000 only creates the Enterprise Admins group in the first domain in the forest. This group initially contains the Administrator account.
- **Schema Admins:** Members of this universal group can modify the Active Directory schema. If you have multiple domains in your forest, Windows 2000 only creates the Schema Admins group in the first domain in the forest. This group initially contains the Administrator account.

Built-in Special Groups Built-in special groups on domain controllers are automatically created during the installation of Active Directory. These built-in special groups are used for specific purposes by the operating system, and are sometimes called system groups.

All of the built-in special groups that exist on nondomain controllers are also present on Windows 2000 domain controllers. The built-in special groups on domain controllers have the same characteristics as the built-in special groups on nondomain controllers. (Built-in special groups on nondomain controllers are covered earlier in this chapter).

Creating Groups in Active Directory

You can create groups in Active Directory by using Active Directory Users and Computers. You must be a member of the domain's built-in local Administrators or Account Operators groups to create groups in Active Directory.

STEP BY STEP

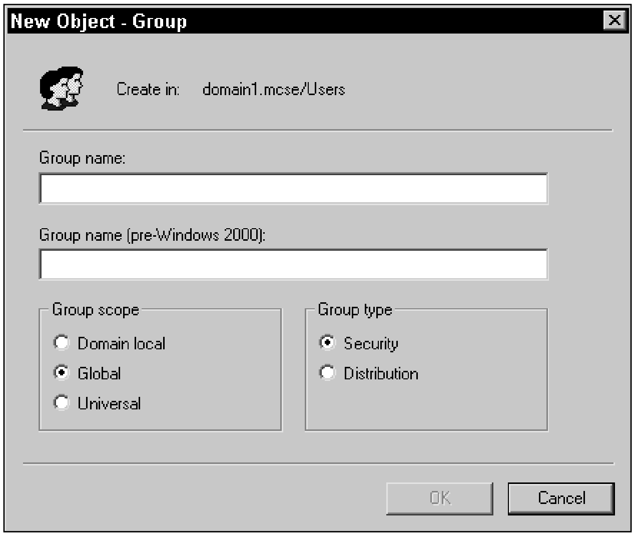
CREATING A GROUP IN ACTIVE DIRECTORY

1. Start Active Directory Users and Computers. (Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.)
2. In the left pane of the Active Directory Users and Computers dialog box, click the + next to the name of the domain in which you want to create a group. Notice the `Users` folder in the domain tree. This folder is the default container in which Windows 2000 places most groups (and all users) that it automatically creates when Active Directory is installed.

   If you have a relatively small organization, you may want to place your administrator-created groups in the `Users` folder, too, so that you can easily locate and administer them.

   Or, if you have a large organization and use OUs to administer groups of users, you can place administrator-created groups in the appropriate OUs.

   Highlight the `Users` folder or the OU in which you want to create a group, and select Action ➪ New ➪ Group.
3. The New Object-Group dialog box appears, as shown in Figure 9-25.



New Object - Group

Create in: domain1.mcse/Users

Group name:

Group name (pre-Windows 2000):

Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution

FIGURE 9-25 Creating a new group

In the “Group name” text box, enter a name for the group.

If you have Windows NT 4.0 computers in your domain, you can assign the group a different name for those computers by entering it in the “Group name (pre-Windows 2000)” text box. If you choose to assign a different name, it should contain 20 characters or fewer for backward compatibility with Windows NT 4.0.

STEP BY STEP *Continued*

Select a group scope — either Domain local, Global, or Universal. The default selection is Global.

TIP

You can't create a universal group in a Windows 2000 domain that is operating in mixed-mode.

Select a group type — either Security or Distribution. The default selection is Security. Click OK.

4. Windows 2000 creates the new group, and displays it in the right pane of the Active Directory Users and Computers dialog box.

Configuring and Managing Group Properties in Active Directory

Once you've created groups in Active Directory, you'll want to add members to these groups and configure various group properties.

You can configure and manage groups in Active Directory by using Active Directory Users and Computers. Members of the Administrators group can fully manage and modify all groups in Active Directory, whereas members of the Account Operators group can manage all groups except the Administrators, Account Operators, Backup Operators, Print Operators, and Server Operators groups.

Some of the most common group management tasks include adding and removing members to and from a group, renaming a group, deleting a group, and configuring group properties.

STEP BY STEP

ADDING MEMBERS TO AND REMOVING MEMBERS FROM A GROUP IN ACTIVE DIRECTORY

1. Start Active Directory Users and Computers. (Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.)
2. In the left pane of the Active Directory Users and Computers dialog box, click the + next to the name of the domain that contains the group you want to add or remove members to or from. Then highlight the `Users` folder or the OU that contains this group. In the right pane, double-click this group.

STEP BY STEP *Continued*

3. In the group's Properties dialog box, click the Members tab.
4. The Members tab appears.

   To *remove* a member from the group, highlight the member in the Members box and click Remove. Then click Yes when Windows 2000 asks if you want to remove the selected member from the group. Skip to Step 6.

   To *add* a member to the group, click Add.
5. The Select Users, Contacts, Computers, or Groups dialog box appears. To add members to this group from the current domain, double-click each user, contact, computer, or group that you want to add.

   If you want to add members to this group from other domains, select the domain from the "Look in" drop-down list box. Then double-click each user, contact, computer, or group that you want to add.

   When you finish adding members to the group, click OK.
6. In the group's Properties dialog box, click OK.

RENAMING OR DELETING A GROUP IN ACTIVE DIRECTORY

1. Start Active Directory Users and Computers. (Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.)
2. In the left pane of the Active Directory Users and Computers dialog box, click the + next to the name of the domain that contains the group you want to rename or delete. Then highlight the `Users` folder or the OU that contains this group. In the right pane, right-click the group you want to rename or delete.

   To *rename* the group, select Rename from the menu that appears, type in a new name for the group, and press Enter. Then click OK in the Rename Group dialog box.

   To *delete* the group, select Delete from the menu that appears. Click Yes when Windows 2000 asks if you're sure you want to delete the group.

TIP

You can't delete any of the domain's built-in groups.

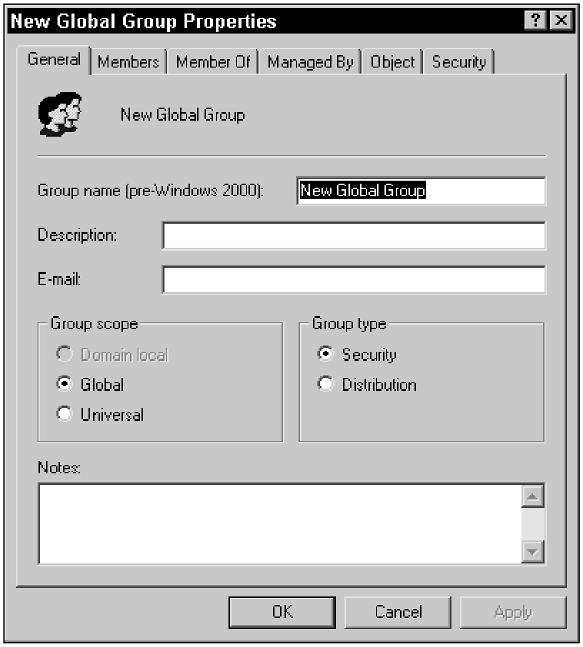
CONFIGURING PROPERTIES OF A GROUP IN ACTIVE DIRECTORY

1. Start Active Directory Users and Computers. (Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.)
2. In the left pane of the Active Directory Users and Computers dialog box, click the + next to the name of the domain that contains the group you want to configure. Then highlight the `Users` folder or the OU that contains this group. In the right pane, double-click this group.

STEP BY STEP

Continued

3. The group's Properties dialog box appears, as shown in Figure 9-26. Notice the six tabs in this dialog box: General, Members, Member Of, Managed By, Object, and Security. (The Object and Security tabs are only displayed when Advanced Features is selected in the View menu.)



New Global Group Properties

New Global Group

Group name (pre-Windows 2000): New Global Group

Description:

E-mail:

Group scope

○ Domain local

● Global

○ Universal

Group type

● Security

○ Distribution

Notes:

FIGURE 9-26 Configuring a group's properties

On the General tab, you can change the group's pre-Windows 2000 name, enter a description for the group, and enter the e-mail address for the group.

On this tab you can also change the group scope. The three possible options are Domain local, Global, and Universal. The actual options available to you will depend on the type of group you're configuring.

You can also change the group type on the General tab. The two possible options are Security and Distribution.

CAUTION

Changing the group scope or group type can significantly change the structure and functionality of the group, including the membership of the group, the resources to which the group can be assigned permissions, and so on. In general, I recommend that you don't change the group scope or group type.

STEP BY STEP *Continued*

Make any appropriate changes on the General tab. If you're finished configuring the group, click OK. Otherwise, I'll explain the other tabs in the following steps.

4. On the Members tab, you can add and remove members to and from the group. (For detailed instructions, see the step-by-step section titled "Adding and removing members to/from a group in Active Directory.")
5. On the Members Of tab, you can add this group to and remove this group from other groups.
6. On the Managed By tab, you can select a user from any domain in Active Directory to be listed as the manager for this group. All of the user's contact information will then be displayed on this tab. To select a user, click Change, and then select a user from the Select User or Contact dialog box. Click OK. If you need to view or modify the user's contact data, click View.
7. On the Object tab, you can view information about the group, including the group's FQDN, the date the group was created, the date the group was last modified, and so on. No configurations are possible on this tab.
8. On the Security tab, you can specify the users and groups that are permitted to view or modify the properties of this group, and assign permissions to these users and groups.
9. When you're finished configuring the group's properties, click OK in the group's Properties dialog box.

KEY POINT SUMMARY

Several important user and group topics were introduced in this chapter:

- User authentication is the process of verifying a user's credentials for the purpose of determining whether the user is permitted to access a local computer or a network resource, such as a shared folder or shared printer.
- There are two Windows 2000 built-in user accounts: Administrator and Guest.
- You can use the Local Users and Groups tool in Computer Management to create and configure local user accounts on a nondomain controller.
- To create and configure domain user accounts in Active Directory, use Active Directory Users and Computers.
- You can also create user accounts by using a batch file or a script file in conjunction with the `NET USER` command-line utility.

- You can copy, rename, and delete user accounts, with the exception of the two built-in accounts, Administrator and Guest, which can't be deleted.
- A user profile is a folder that contains a collection of settings and options that specify a user's desktop and all other user-definable settings for a user's work environment. The System application in Control Panel is used to copy user profiles.
- Roaming user profiles are user profiles that are stored on a Windows 2000 Server computer. Because these profiles are stored on a server, they are available to users regardless of which Windows 2000 computer on the network they log on to.
- A mandatory user profile is a user profile that, when assigned to a user, can't be changed by the user. A user can make changes to desktop and work environment settings during a single logon session, but these changes are *not* saved to the mandatory user profile when the user logs off.
- Windows 2000 account policies are sets of rules that are applied to many user accounts, often to all of the users in a domain. There are three major types of account policies: password policy, account lockout policy, and Kerberos policy.
- User rights authorize individual users and groups to perform specific tasks. User rights are *not* the same as permissions: user rights enable users to perform tasks; whereas permissions enable users to access objects, such as files, folders, printers, and Active Directory objects.
- Groups on the local computer are primarily used to control access to resources on that computer. All groups on the local computer are security groups. There are two kinds of groups found on the local computer: local groups and built-in groups.
- You can create and manage local groups by using the Local Users and Groups tool in Computer Management. You must be a member of the Administrators, Power Users, or Users groups to create a local group.
- Groups in Active Directory are used to control access to network resources and to organize users who perform similar job tasks and/or have similar network access requirements.
- There are three administrator-created kinds of groups in Active Directory: domain local groups, global groups, and universal groups. In addition, there are built-in local, global, universal, and special groups in Active Directory.

- You can create groups in Active Directory by using Active Directory Users and Computers. You must be a member of the domain's built-in local Administrators or Account Operators groups to create groups in Active Directory.

STUDY GUIDE

This section contains several exercises designed to drive home the user and group concepts presented in this chapter:

- **Assessment questions:** These questions test your knowledge of the user and group topics covered in this chapter. You can find the answers to these questions at the end of this chapter.
- **Scenario:** The situation-based questions in scenarios challenge you to apply your understanding of the material to solve a hypothetical problem. In this chapter's scenario, you are asked to describe the action you would take to solve a number of given troubleshooting problems. You don't need to be at a computer to do scenarios. Answers to this chapter's scenario are presented at the end of this chapter.
- **Lab Exercises:** These exercises are hands-on practice activities that you perform on a Windows 2000 computer. The two labs in this chapter give you an opportunity to create local and domain user and group accounts; test local user authentication; and work with account policies, user rights, and user profiles.

Assessment Questions

1. You want to create a local user account on a Windows 2000 computer. Which tool should you use?
   - A. Local Security Policy
   - B. Local Users and Groups
   - C. The System application
   - D. Active Directory Users and Computers
2. You want to create a domain user account. Which tool should you use?
   - A. Users and Passwords
   - B. The System application
   - C. Local Users and Groups
   - D. Active Directory Users and Computers

3. You want to assign a roaming user profile to a user. Where should you store this user's profile folder?

   A. In the `C:\Documents and Settings\`*`user_name`* folder on the local computer

   B. In the `All Users` profile folder on the local computer

   C. In a shared folder on a Windows 2000 Server computer

   D. In the `Default User` profile folder on a Windows 2000 Server computer

4. You want to assign a mandatory user profile to a user. What must you do?

   A. Rename the user's `NTUSER.DAT` file.

   B. Rename the user's `ntuser.ini` file.

   C. Copy the `Default User` profile folder to the user's profile folder.

   D. Copy the user's profile folder to the `Default User` profile folder.

5. You want to copy a user profile. What tool should you use?

   A. Windows Explorer

   B. The System application

   C. Local Users and Groups

   D. Active Directory Users and Computers

6. You want all of the users on your Windows 2000 network to use passwords that are at least eight characters long. You also want all users to use two different passwords before an old password can be reused. Which account policies should you configure?

   A. "Enforce password history" and "Minimum password age"

   B. "Maximum password age" and "Minimum password length"

   C. "Enforce password history" and "Minimum password length"

   D. "Minimum password length" and "Passwords must meet complexity requirements"

7. You want to configure a newly created local group on the local Windows 2000 computer. Which tool should you use?

   A. Local Security Policy

   B. Local Users and Groups

   C. The System application

   D. Active Directory Users and Computers

8. You want to create a domain local group. Which tool should you use?
   - A. Local Security Policy
   - B. Domain Security Policy
   - C. Local Users and Groups
   - D. Active Directory Users and Computers
9. Your company has 50 sales representatives. The domain user accounts of these sales representatives are the only members of a single global group. You want to assign all of the sales representatives permissions to a specific printer located in the sales office. How can you efficiently accomplish this?
   - A. Assign each of the sales representatives' user accounts permissions to the printer.
   - B. Create a new global group. Make the user accounts of all of the sales representatives members of the new global group. Assign permissions to the printer to the new global group.
   - C. Create a new built-in special group. Assign permissions to the printer to the built-in special group. Make the global group that contains the sales representatives a member of the new built-in special group.
   - D. Create a new domain local group. Assign permissions to the printer to the new domain local group. Make the global group that contains the sales representatives a member of the new domain local group.
10. You want to use a single group to organize users from multiple domains that perform similar job tasks. Which kind of group should you use?
    - A. Universal group
    - B. Global group
    - C. Domain local group
    - D. Built-in special group

Scenarios

The following scenarios provide you with an opportunity to apply the knowledge you've gained in this chapter about troubleshooting local and domain user accounts. User account problems can arise due to a number of different causes. For each of the following problems, consider the given situation and facts, and state what course of action you would take to try to resolve the problem.

1. A user, ToddE, reports that he can't log on to his Windows 2000 computer. Windows 2000 displayed the following message: "Your account has been disabled. Please see your system administrator."
2. A user, SusanB, usually works from Monday through Friday. However, this past weekend she came in to work and could not log on to her Windows 2000 computer. Windows 2000 displayed the following message: "Unable to log you on because of an account restriction."
3. A user, AnneC, reports that Windows 2000 prompted her to change her password, but when she typed in a new password, Windows 2000 would not accept the new password. Windows 2000 displayed the following message: "Your password must be at least 9 characters; cannot repeat any of your previous 3 passwords; must contain capitals, numerals, or punctuation . . ."
4. A user, JeffT, reports that he can't log on locally to your network's Windows 2000 domain controller.
5. A user, GregZ, reports that he is unable to log on to his Windows 2000 computer. Windows 2000 displayed the following message: "The system could not log you on."

Lab Exercises

These labs are designed to provide you with hands-on experience working with users and groups in a Windows 2000 environment.

Lab 9-1 Implementing local user authentication and local users and groups

▶ Professional
▶ Server

The purpose of this lab is to give you practical experience working with local users and groups on a Windows 2000 Professional computer.

There are three parts to this lab:

- Part 1: Creating and Configuring Local Users and Groups
- Part 2: Implementing and Configuring User Rights
- Part 3: Testing Local User Authentication

Begin this lab by booting your computer to Windows 2000 Professional and logging on as Administrator.

Part 1: Creating and Configuring Local Users and Groups

In this part, you use Local Users and Groups to create two local user accounts and configure account settings. You also create and configure a group on the local computer, and place your two new users in groups.

1. From the desktop, right-click My Computer, and select Manage from the menu that appears.
2. In the Computer Management dialog box, click the + next to Local Users and Groups. Highlight the `Users` folder, and select Action ➪ New User.
3. The New User dialog box appears. Type **User1** in the "User name" text box. Type **Regular User** in the "Full name" text box. Type **newuser** in the Password text box. Confirm the password by retyping it. Click Create.
4. The New User dialog box reappears. Type **Backup** in the "User name" text box. Type **Backup User** in the "Full name" text box. Type **Can only backup files** in the Description text box. Type **password** in the Password text box. Confirm the password by retyping it. Clear the check box next to "User must change password at next logon." Select the check box next to "User cannot change password" and "Password never expires." Click Create.

5. In the New User dialog box, click Close. The new users are created, and appear in the right pane of the Computer Management dialog box. In the right pane, double-click User1.
6. In the User1 Properties dialog box, click the Profile tab.
7. On the Profile tab, type **C:\User1** in the "Profile path" text box. Click OK.
8. In the left pane of the Computer Management dialog box, highlight the `Groups` folder. Select Action ➪ New Group.
9. In the New Group dialog box, type **Backuponly** in the "Group name" text box. Enter a description of **Members can back up files but not restore them**. Click Add.
10. In the Select Users or Groups dialog box, scroll down until the user named Backup is displayed. Double-click Backup. Click OK.
11. In the New Group dialog box, click Create. Then click Close.
12. In the right pane of the Computer Management dialog box, double-click Power Users.
13. In the Power Users Properties dialog box, click Add.
14. In the Select Users or Groups dialog box, scroll down until the user named User1 is displayed. Double-click User1. Click OK.
15. In the Power Users Properties dialog box, click OK.
16. Close Computer Management.

Part 2: Implementing and Configuring User Rights

In this part, you use the Local Security Policy tool to assign user rights to the group you created in Part 1.

1. Select Start ➪ Settings ➪ Control Panel.
2. In the Control Panel dialog box, double-click Administrative Tools.
3. In the Administrative Tools dialog box, double-click Local Security Policy.
4. In the left pane of the Local Security Settings dialog box, click the + next to Local Policies. In the left pane, highlight User Rights Assignment. In the right pane, double-click the "Log on locally" user right.
5. In the Local Security Policy Setting dialog box, click Add.

6. In the Select Users or Groups dialog box, scroll down until the Backuponly group is displayed. Double-click Backuponly. Click OK.
7. In the Local Security Policy Setting dialog box, click OK.
8. In the right pane of the Local Security Settings dialog box, double-click the "Back up files and directories" user right.
9. In the Local Security Policy Setting dialog box, click Add.
10. In the Select Users or Groups dialog box, scroll down until the Backuponly group is displayed. Double-click Backuponly. Click OK.
11. In the Local Security Policy Setting dialog box, click OK.
12. Close the Local Security Settings dialog box.
13. Close Administrative Tools.

Part 3: Testing Local User Authentication

In this part, you test local user authentication by logging on as one of the users you created in Part 1.

1. From the desktop, select Start ➪ Shut Down.
2. In the Shut Down Windows dialog box, select "Log off administrator" from the drop-down list box. Click OK.
3. In the Log On to Windows dialog box, enter a User name of User1, and a password of **wrongo**, and click OK.
4. A Logon Message appears, indicating that the system could not log you on. Local user authentication failed because you entered an incorrect user password. Click OK.
5. In the Log On to Windows dialog box, enter a password of **newuser**, and click OK.
6. A Logon Message appears, indicating that you must change your password. (Remember that when you created this user, you accepted the default selection of "User must change password at next logon.") Click OK.
7. In the Change Password dialog box, type **password** in the New Password text box, and confirm the new password by retyping it. Click OK.
8. A Change Password dialog box appears, indicating that your password has been changed. Click OK.

9. Windows 2000 logs you on as User1. You have successfully authenticated to Windows 2000 by using a local user account. Shut down your computer, reboot it to Windows 2000 Server, and log on as Administrator to do the next lab.

Lab 9-2 Implementing domain user and group accounts, account policies, user rights, and user profiles

MCSE EXAM MATERIAL

- ▶ Professional
- ▶ Server
- ▶ Directory Services

The purpose of this lab is to give you practical experience working with domain users and groups on a Windows 2000 Server computer.

There are four parts to this lab:

- Part 1: Configuring Account Policies and Assigning User Rights
- Part 2: Creating and Configuring Domain User and Group Accounts
- Part 3: Creating and Configuring Domain User Accounts by Scripting
- Part 4: Configuring and Managing User Profiles

Begin this lab by booting your computer to Windows 2000 Server and logging on as Administrator.

Part 1: Configuring Account Policies and Assigning User Rights

In this part, you use the Domain Security Policy tool to configure account policies (including password policy and account lockout policy) and to assign a user right.

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Domain Security Policy.
2. In the left pane of the Domain Security Policy dialog box, click the + next to Security Settings. Then click the + next to Account Policies. Highlight Password Policy.
3. In the right pane, double-click "Enforce password history."

4. In the Security Policy Setting dialog box, configure the "Keep password history" spin box to 8 passwords remembered. Click OK.
5. In the right pane of the Domain Security Policy dialog box, double-click "Maximum password age."
6. In the Security Policy Setting dialog box configure the "Passwords expire in" spin box to 30 days. Click OK.
7. If a Suggested Value Changes dialog box appears, click OK.
8. In the right pane of the Domain Security Policy dialog box, double-click "Minimum password age."
9. In the Security Policy Setting dialog box, configure the "Passwords can be changed after" spin box to 5 days. Click OK.
10. In the right pane of the Domain Security Policy dialog box, double-click "Minimum password length."
11. In the Security Policy Setting dialog box, configure the "No password required" spin box to 8 characters. (Note that the name of this spin box changes to "Password must be at least.") Click OK.
12. In the left pane of the Domain Security Policy dialog box, highlight Account Lockout Policy.
13. In the right pane, double-click "Account lockout threshold."
14. In the Security Policy Setting dialog box configure the "Account will not lock out" spin box to 3 invalid logon attempts. (Note that the name of this spin box changes to "Account will lock out after.") Click OK.
15. In the Suggested Value Changes dialog box, click OK.
16. In the left pane of the Domain Security Policy dialog box, click the + next to Local Policies. In the left pane, highlight User Rights Assignment. In the right pane, double-click the "Log on locally" user right.
17. In the Security Policy Setting dialog box, select the check box next to "Define these policy settings." Click Add.
18. In the "Add user or group" dialog box, click Browse.
19. In the Select Users or Groups dialog box, scroll down until the Everyone group is displayed. Double-click Everyone. Click OK.
20. In the "Add user or group" dialog box, click OK.
21. In the Security Policy Setting dialog box, click OK.
22. Close Domain Security Policy.

IN THE REAL WORLD

You have just assigned the “Log on locally” user right to the Everyone group for all computers in the domain. This is *not* typically done in the real world, but is necessary for you to complete the labs in this book because your lab computer is a Windows 2000 domain controller.

Part 2: Creating and Configuring Domain User and Group Accounts

In this part, you use Windows Explorer to create and share a folder that will contain roaming user profiles. Then you use Active Directory Users and Computers to create and configure several domain user and group accounts. Finally, you assign users to groups.

1. From the desktop, right-click My Computer, and select Explore from the menu that appears.
2. In the left pane of the My Computer dialog box, highlight Local Disk (C:). Select File ➪ New ➪ Folder.
3. In the right pane, type in a new folder name of **Profiles** and press Enter. In the right pane, right-click the `Profiles` folder, and select Sharing from the menu that appears.
4. In the Profiles Properties dialog box, select the “Share this folder” option. Click OK. You’ve now created and shared a folder that will contain roaming user profiles.
5. Close Windows Explorer.
6. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.
7. In the left pane of the Active Directory Users and Computers dialog box, click the + next to domain1.mcse. Click the + next to the HQ Seattle OU.
8. Highlight the Accounting OU, and select Action ➪ New ➪ User.
9. In the New Object - User dialog box, enter the following information:

   First name: **Robert**

   Last name: **Jones**

   User logon name: **RobertJ**

   Click next.

10. In the New Object - User dialog box, enter a password of **changeme**, and confirm this password by retyping it. Select the check box next to "User must change password at next logon." Click Next.
11. In the New Object - User dialog box, click Finish.
12. Repeat Steps 8 through 11 to create two additional new users in the Accounting OU. When prompted, enter the following information for the additional new users:

Text Box Label	1st Additional User	2nd Additional User
First name	**Nancy**	**Mike**
Last name	**Yates**	**Cook**
User logon name	**NancyY**	**MikeC**
Password	**changeme**	**changeme**

13. In the left pane of the Active Directory Users and Computers dialog box, highlight the Information Services OU, and select Action ➪ New ➪ User.
14. In the New Object - User dialog box, enter the following information:

    First name: **Mike**

    Last name: **Calhoun**

    User logon name: **MikeCa**

    Click next.
15. In the New Object - User dialog box, enter a password of **changeme**, and confirm this password by retyping it. Select the check box next to "User must change password at next logon." Click Next.
16. In the New Object - User dialog box, click Finish.
17. In the left pane of the Active Directory Users and Computers dialog box, highlight the Marketing OU, and select Action ➪ New ➪ User.
18. In the New Object - User dialog box, enter the following information:

    First name: **Pam**

    Last name: **Rhodes**

    User logon name: **PamR**

    Click next.

19. In the New Object - User dialog box, enter a password of **changeme**, and confirm this password by retyping it. Select the check box next to "User must change password at next logon." Click Next.
20. In the New Object - User dialog box, click Finish.
21. Repeat Steps 17 through 20 to create three additional new users in the Marketing OU. When prompted, enter the following information for the additional new users:

Text Box Label	1st New User	2nd New User	3rd New User
First name	**John**	**Colleen**	**Bill**
Last name	**Spencer**	**Green**	**Tracy**
User logon name	**JohnS**	**ColleenG**	**BillT**
Password	**changeme**	**changeme**	**changeme**

22. In the left pane of the Active Directory Users and Computers dialog box, highlight the Accounting OU. Then, in the right pane, double-click Robert Jones.
23. On the General tab in the Robert Jones Properties dialog box, type **Accounting Manager** in the Description text box. Click the Profile tab.
24. On the Profile tab, type **\\Server01\Profiles\RobertJ** in the Profile path text box. Click OK.
25. Repeat Steps 22 through 24 to configure account settings for each of the new domain users you created. Remember to highlight the appropriate OU to access each user account. Use the following table to assign a description and profile path to each user.

OU	User	Description	Profile Path
Accounting	Nancy Yates	**Accounting Staff**	**\\Server01\Profiles\NancyY**
Accounting	Mike Cook	**Accounting Staff**	**\\Server01\Profiles\MikeC**
Information Services	Mike Calhoun	**Information Services Manager**	**\\Server01\Profiles\MikeCa**

OU	User	Description	Profile Path
Marketing	Pam Rhodes	**District Manager**	**\\Server01\Profiles\PamR**
Marketing	John Spencer	**Sales Manager**	**\\Server01\Profiles\JohnS**
Marketing	Colleen Green	**Sales Rep**	**\\Server01\Profiles\ColleenG**
Marketing	Bill Tracy	**Sales Rep**	**\\Server01\Profiles\BillT**

26. In the left pane of the Active Directory Users and Computers dialog box, highlight the Accounting OU.
27. Select Action ➪ New Group.
28. In the New Object - Group dialog box, enter/configure the following information for the new group:

    Group name: **Accountants**

    Group scope: **Global**

    Group type: **Security**

    Click OK.
29. In the right pane of the Active Directory Users and Computers dialog box, double-click the group you just created.
30. On the General tab in the group's Properties dialog box, type **Accounting Managers and Staff** in the Description text box. Click the Members tab.
31. On the Members tab, click Add.
32. In the Select Users, Contacts, Computers, or Groups dialog box, add the following users to the group by double-clicking each user: Pam Rhodes, Robert Jones, Nancy Yates, and Mike Cook. Then click OK.
33. In the group's Properties dialog box, click OK.
34. In the left pane of the Active Directory Users and Computers dialog box, highlight the Marketing OU. Then repeat Steps 27 through 33 two more times to create and configure two additional groups. Use the information in the following table to help you create these two groups.

Configurable Options	1st Additional Group	2nd Additional Group
Group name	**Sales**	**Managers**
Group scope	**Global**	**Global**
Group type	**Security**	**Security**
Description	**Sales Managers and Representatives**	**Corporate Managers**
Members to be added to group	**Pam Rhodes, John Spencer, Colleen Green, Bill Tracy**	**Pam Rhodes, John Spencer, Robert Jones, Mike Calhoun**

35. In the left pane of the Active Directory Users and Computers dialog box, highlight the `Users` folder. In the right pane, double-click the Enterprise Admins group.
36. In the Enterprise Admins Properties dialog box, click the Members tab.
37. On the Members tab, click Add.
38. In the Select Users, Contacts, Computers, or Groups dialog box, scroll down until Mike Calhoun is displayed. Double-click Mike Calhoun. Click OK.
39. In the Enterprise Admins Properties dialog box, click OK. You have just made Mike Calhoun (the Information Services Manager) a member of the Enterprise Admins group so that he can administer Active Directory and all computers in the domain. Close Active Directory Users and Computers.

Part 3: Creating and Configuring Domain User Accounts by Scripting

In this part, you use Notepad and the `NET USER` and `NET GROUP` command-line utilities to create a script file. Then you use this script file to create two new domain users and assign these users to the Domain Admins group.

1. From the desktop, select Start ➪ Programs ➪ Accessories ➪ Notepad.
2. In the Untitled - Notepad dialog box, enter the following three lines of text. (Press Enter after you type each line.)

```
net user SteveS password /add /fullname:”Steve Smith” /domain
net user PeteS password /add /fullname:”Pete Short” /domain
net group “domain admins” SteveS PeteS /add /domain
```

Select File ➪ Save As.

3. In the Save As dialog box, type **C:\newusers.bat** in the “File name” text box. Select “All Files” from the “Save as type” drop-down list box. Click Save.
4. Close Notepad.
5. Select Start ➪ Run.
6. In the Run dialog box, type **C:\newusers.bat** in the Open text box. Click OK. Windows 2000 creates the two new users and adds them to the Domain Admins group.
7. Start Active Directory Users and Computers. (Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.)
8. In the left pane of the Active Directory Users and Computers dialog box, click the + next to domain1.mcse (if it is not already expanded). Highlight the Users folder. In the right pane, scroll down until the new users you just created (PeteS and SteveS) are displayed. Then scroll up until the Domain Admins group is displayed. Double-click Domain Admins.
9. In the Domain Admins Properties dialog box, click the Members tab.
10. On the Members tab, notice that both PeteS and SteveS are listed as members of the Domain Admins group. Click OK.
11. Close Active Directory Users and Computers.

Part 4: Configuring and Managing User Profiles

In this part, you log on as one of the new users you created in Part 3. Then you customize the user’s profile, copy the customized user profile to the `Default User` profile folder, and assign a mandatory user profile to a user.

1. From the desktop, select Start ➪ Shut Down.
2. In the Shut Down Windows dialog box, select “Log off administrator” from the drop-down list box. Click OK.
3. Press Ctrl+Alt+Delete.
4. In the Log On to Windows dialog box, enter a user name of **SteveS** and a password of **password**. Click OK.
5. In the Windows 2000 Configure Your Server dialog box, clear the check box next to “Show this screen at startup”. Close the Windows 2000 Configure Your Server dialog box.

6. Right-click the desktop, and select Properties from the menu that appears.
7. On the Background tab in the Display Properties dialog box, select a wallpaper of Snow Trees from the scrolling list box. Click OK.
8. Click Yes to enable Active Desktop.
9. Right-click the desktop, and select New ➪ Shortcut from the menu that appears.
10. In the Create Shortcut dialog box, type **calc.exe** in the text box. Click Next.
11. In the Select a Title for the Program dialog box, type **Calculator** in the text box. Click Finish. The shortcut to the calculator appears on the desktop.
12. From the desktop, select Start ➪ Shut Down.
13. In the Shut Down Windows dialog box, select "Log off SteveS" from the drop-down list box. Click OK.
14. Press Ctrl+Alt+Delete.
15. In the Log On to Windows dialog box, enter a user name of **Administrator** and a password of **password**. Click OK.
16. Right-click My Computer, and select Properties from the menu that appears.
17. In the System Properties dialog box, click the User Profiles tab.
18. On the User Profiles tab, highlight the DOMAIN1\SteveS profile and click Copy To.
19. In the Copy To dialog box, type **C:\Winnt\Sysvol\Sysvol\domain1.mcse\Scripts\Default User** in the "Copy profile to" text box. Click Change.
20. In the Select User or Group dialog box, type **Everyone** in the Name text box. Click OK.
21. In the Copy To dialog box, click OK. You have just modified the domain-wide `Default User` profile folder.
22. In the System Properties dialog box, highlight the DOMAIN1\SteveS profile and click Copy To.
23. In the Copy To dialog box, type **\\Server01\Profiles\BillT** in the "Copy profile to" text box. Click Change.

24. In the Select User or Group dialog box, scroll down until the user Bill Tracy is displayed. Double-click Bill Tracy.
25. In the Copy To dialog box, click OK. You've just copied Steve Smith's user profile to Bill Tracy's profile folder.
26. In the System Properties dialog box, click OK.
27. Right-click My Computer, and select Explore from the menu that appears.
28. In the left pane of the My Computer dialog box, click the + next to Local Disk (C:). Highlight the `Profiles` folder. In the right pane, double-click the `BillT` folder. Select Tools ➪ Folder Options.
29. In the Folder Options dialog box, click the View tab.
30. On the View tab, select the option next to "Show hidden files and folders." Clear the check box next to "Hide file extensions for known file types." Click OK.
31. In the right pane of the BillT dialog box, right-click the `ntuser.dat` file, and select Rename from the menu that appears.
32. Type in a new name for the file of **ntuser.man** and press Enter. You have just configured BillT's profile to be a mandatory user profile. Close Windows Explorer.

Answers to Chapter Questions

Chapter Pre-Test

1. Kerberos V5 is an Internet standard authentication protocol that provides a higher level of security and faster, more efficient authentication than the Windows NT LAN Manager protocol. Kerberos V5 is the default protocol used between Windows 2000 computers when each of these computers is a member of a Windows 2000 domain.
2. The two Windows 2000 built-in user accounts are Administrator and Guest.
3. Local user accounts enable users to log on to the local computer and to access that computer's resources. Domain user accounts enable users to log on to the domain and to access resources in the domain.

4. Roaming user profiles are user profiles that are stored on a Windows 2000 Server computer. Because these profiles are stored on a server instead of on the local computer, they are available to users regardless of which Windows 2000 computer on the network they log on to.

   A mandatory user profile is a user profile that, when assigned to a user, can't be changed by the user. A user can make changes to desktop and work environment settings during a single logon session, but these changes are *not* saved to the mandatory user profile when the user logs off.
5. The three major types of Windows 2000 account policies are: password policy, account lockout policy, and Kerberos policy.
6. Security groups are primarily used to assign permissions and user rights to multiple users. Distribution groups are primarily used to send e-mail messages to a specified list of users. You can't assign permissions and user rights to distribution groups.
7. A built-in group

Assessment Questions

1. **B.** Use the Local Users and Groups tool in Computer management to create a new local user account on the local Windows 2000 computer.
2. **D.** Use Active Directory Users and Computers to create a new domain user account.
3. **C.** Roaming user profiles are server-based profiles. They should be stored in a shared folder on a Windows 2000 Server computer.
4. **A.** To make a user's profile mandatory, you must rename the user's `NTUSER.DAT` file as `NTUSER.MAN`.
5. **B.** Use the System application (found in Control Panel) to copy user profiles — you can't use Windows Explorer for this task.
6. **C.** "Enforce password history" requires that a certain number of different passwords be used before an old password can be reused (in this case, two). "Minimum password length" specifies the minimum number of characters a password can contain (in this case, eight).
7. **B.** Use Local Users and Groups to create and configure local groups on the local Windows 2000 computer.

8. **D.** Use Active Directory Users and Computers to create and configure groups in Active Directory, such as a domain local group.
9. **D.** Answer A will work, but is not correct because it is not efficient. Answer B will also work, but again, is not correct because it is not efficient and is not the manner in which global groups are typically used. Answer C is incorrect because built-in groups can't be created by an administrator, nor can you add users and groups to built-in special groups. Answer D is the best solution, and is the manner in which domain local and global groups are typically used.
10. **A.** Universal groups are used to organize users from multiple domains that perform similar job tasks or have similar network access requirements, and/or to control access to shared resources in multiple domains.

Scenarios

1. This message is displayed when a local user's account has been locked out or has been disabled. On the General tab in the local user's Properties dialog box, clear the check box next to "Account is locked out" or clear the check box next to "Account is disabled."
2. This message is displayed when a user attempts to log on during restricted hours or attempts to log on to a restricted computer. Check the Logon Hours and Log On To settings on the Account tab in the user's Properties dialog box, and make any necessary changes.
3. Examine the Password Policy settings. Check to see if the new password the user has entered meets the minimum password length and password complexity requirements. Remember, if password complexity is enabled, the password must contain three of the four types of characters: uppercase alphabetic, lowercase alphabetic, numbers, and special characters. Is the user's new password a password that she has used previously? If so, check to see if it meets the "Enforce password history" settings.

4. By default, only Administrators can log on locally to the domain controller. Restricting local logon to the domain controller is generally a preferred practice. Use the Domain Controller Security Policy tool to grant the user the "Log on locally" user right, or make the user a member of a group that has that user right. Remember, if the user has been assigned both the "Log on locally" and "Deny logon locally" user rights, the "Deny logon locally" right takes precedence.
5. Verify that the user name and password the user is using are correct. Remember, passwords are case sensitive. Make sure that Caps Lock is not on.