Workstation
Server
Enterprise

CHAPTER

Managing User and Group Accounts

7

About Chapter 7

This chapter could be called, "Everything You Always Wanted to Know About Users and Groups but Were Afraid Someone Would Explain to You in Great Detail."

It starts by taking you through the steps to create a user account, including important tips on naming conventions and passwords. Then it outlines how to configure specific Windows NT user account properties. Other common user account tasks are also explained, including how to copy user accounts, how to apply properties to multiple user accounts, and how to rename and delete user accounts.

The remainder of this chapter focuses on creating and managing groups. Local groups and global groups are discussed and compared extensively. You'll not only find out how to create these groups but also how and when to use them to efficiently organize users and to assign rights and permissions to multiple users. Built-in groups and special groups are also addressed.

This chapter includes one comprehensive hands-on lab. You'll practice creating user accounts, managing user account properties, creating group accounts, assigning user accounts to groups, and creating user account templates.

Chapter 7 is a "must read" no matter which of the three Windows NT 4.0 Microsoft Certified Professional exams you're preparing for. This chapter maps to the "Manage user and group accounts" objective in the Managing Resources section in these exams' objectives.

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 NT computers or domains.

There are two types of user accounts: built-in accounts, and user accounts that you create. You can configure various user account properties, including group memberships, profile, logon script, logon hours, workstation logon restrictions, account expiration, and dialin permission.

The following sections cover these topics, as well as copying user accounts, applying properties to multiple accounts, and renaming and deleting user accounts.

Built-in User Accounts

There are two built-in user accounts in Windows NT: *Administrator* and *Guest*. Built-in accounts are created automatically during the installation of Windows NT.

The Administrator account has all of the rights and permissions needed to fully administer a Windows NT computer or a Windows NT domain. The Administrator account can be used to perform numerous tasks, including creating and managing users and groups, managing file and folder permissions, and installing and managing printers and printer security. In addition, members of the Administrators local group have the right to take ownership of any file, folder, or printer. The Administrator account's rights and permissions are due solely to its membership in the Administrators local group.

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. (Renaming user accounts is covered later in this chapter.)

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

The Guest account is disabled by default. If your network contains sensitive data I recommend, for security reasons, you leave the Guest account disabled. Instead of using the Guest account, establish a user account for every person who needs access to network resources.

Creating a User Account

Every person who uses the network should have a user account. You can create user accounts by using User Manager (on a Windows NT Workstation computer) or User Manager for Domains (on a Windows NT Server computer).

TO CREATE A USER ACCOUNT, FOLLOW THESE STEPS:

1. Select Start ≥ Programs ≥ Administrative Tools (Common) ≥ User Manager (or User Manager for Domains).

2. In the User Manager dialog box, select User ➢ New User.
3. The New User dialog box, shown in Figure 7-1, appears. Fill in the user name, person's full name (optional), description (this could be a department, location, or job title—it is also optional), and password. Confirm the password by retyping it.

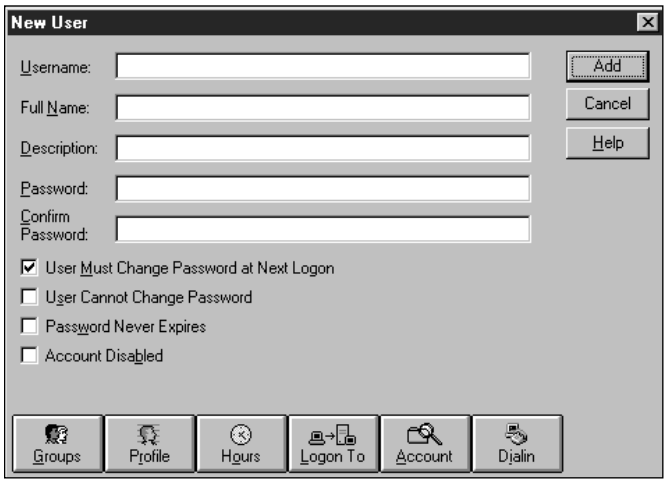


FIGURE 7-1 **Creating a user account**

4. Select the check box next to 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. This option is selected by default.

   Select the check box next to User Cannot Change Password if you—the network administrator—want to manage user passwords.

   Select the check box next to Password Never Expires if you are configuring a user account for a Windows NT service to use when it logs in.

   Select the check box next to Account Disabled if you are creating a user template.
5. Use the command buttons at the bottom of the New User dialog box to configure group memberships, profile and home folder location, logon hours, logon restrictions, and dialin permission for the new user account. (These options are each discussed in detail later in this chapter.)
6. Click the Add command button. Click the Close command button. The new user account is created.

Naming conventions

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

- User account names can be from one to twenty characters long.
- User account names created in a domain must be unique within the domain. User account names created on a non-domain controller (such as a stand-alone server) must be unique within the non-domain controller.
- User account names cannot be the same as a group name within the domain or non-domain controller.
- The following characters may *not* be used in user account names: < > ? * + , = | ; : [ ] \ / “

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 several possible naming schemes you can use. Often, the overall length of a user account name is limited to eight characters (to be compatible with MS-DOS directory name limitations), although this is not mandatory. Common naming schemes 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 above schemes

Table 7-1 shows how three user account names would appear using the naming conventions described in A, B, and C above.

TABLE 7-1 USER ACCOUNT NAMING CONVENTIONS

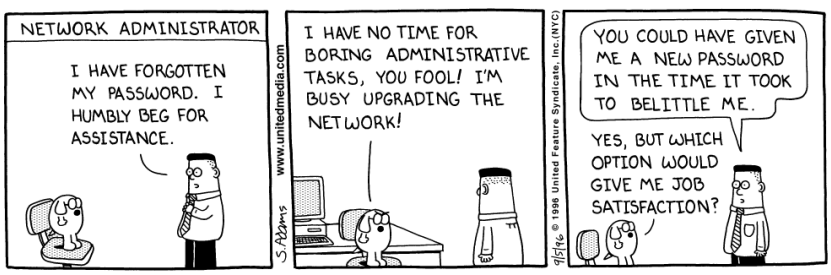
FULL NAME	*SCHEME A*	*SCHEME B*	*SCHEME C*
Nancy Yates	NancyY	Nyates	NY5500
Robert Jones	RobertJ	Rjones	RJ1234
Jonathan Whitmore	JonathaW	Jwhitmor	JW2266

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 you choose to adopt the naming convention described in A above, you would need to have a way to resolve potential duplicate user names. You could resolve the problem by assigning Mike Smith the user account name of MikeS (assuming he was hired before Mike Sutherland), and assigning Mike Sutherland the user account name of MikeSu.

Passwords

Just 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?



DILBERT reprinted by permission of United Feature Syndicate, Inc.

in the real world

I almost never recommend that the network administrator maintain user passwords, because it can take an enormous amount of administrator time to maintain passwords for users.

Normally the only time a network administrator should maintain user passwords is when the highest level of network security is required. The administrator can then assign passwords of the 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 names of family members or pets as passwords. (This is a common security loophole on most networks.)

- Never disclose your password to anyone. Don't write your password on a sticky note and stick it to 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 a password, the more difficult it is to guess. The maximum password length is fourteen characters.
- Use a mix of upper- and lowercase letters, numbers, and special characters. Remember, passwords are case-sensitive.
- If passwords are 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 know several network administrators who actually do this.)

User Account Properties

User accounts have numerous options that can be configured. These options are called *user account properties.*

User account properties that you can configure include group memberships, profile, logon scripts, logon hours, workstation logon restrictions, account expiration, and dialin permission.

User account properties are configured in the User Properties dialog box in User Manager (on a Windows NT Workstation computer) or in User Manager for Domains (on a Windows NT Server computer).

Figure 7-2 shows the User Properties dialog box for Administrator in User Manager (or User Manager for Domains) on a Windows NT computer configured as a non-domain controller. *Non-domain controllers* include Windows NT Workstation computers and Windows NT Server computers configured as stand-alone or member servers. Notice the Groups, Profile, and Dialin command buttons along the bottom of the dialog box.

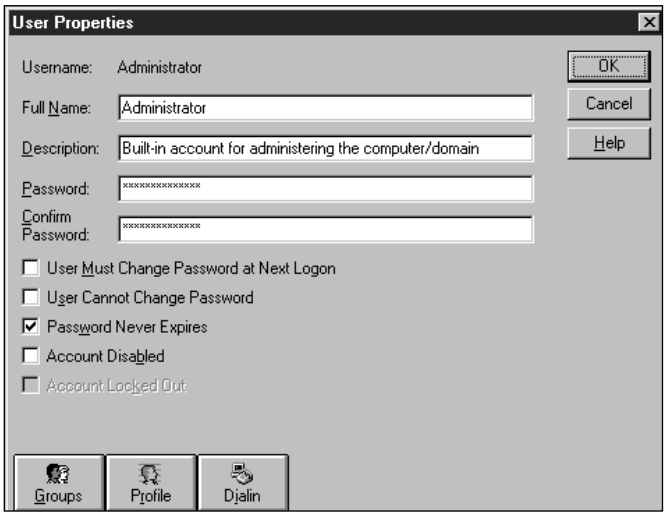


FIGURE 7-2 **Administrator's user properties on a non-domain controller**

Figure 7-3 shows the User Properties dialog box for Administrator in User Manager for Domains on a Windows NT Server computer configured as a primary domain controller (PDC). Notice the Groups, Profile, Hours, Logon To, Account, and Dialin command buttons along the bottom of the dialog box. More account properties can be configured on a domain controller than on a non-domain controller.

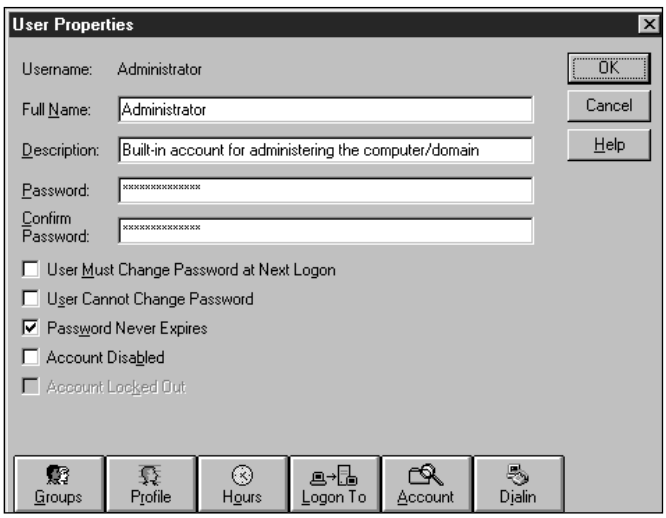


FIGURE 7-3 **Administrator's user properties on a domain controller**

TO ACCESS THE USER PROPERTIES DIALOG BOX, FOLLOW THESE STEPS:

1. Select Start ≥ Programs ≥ Administrative Tools (Common) ≥ User Manager or User Manager for Domains.
2. In the User Manager dialog box, double-click any user name in the Username list box.

Groups

The Groups command button in the User Properties dialog box is used to configure which group(s) a user is a member of. Assigning users to groups is an efficient way to manage permissions for multiple users. (The subject of groups is covered in more detail later in this chapter.)

When you click the Groups command button in the User Properties dialog box, the Group Memberships dialog box appears. Figure 7-4 shows the Group Memberships dialog box for Administrator.

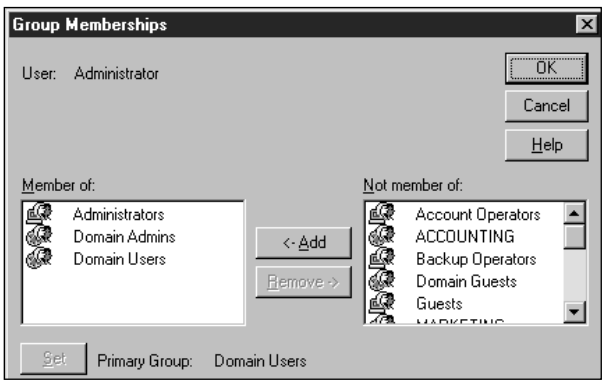


FIGURE 7-4 Administrator's group memberships

To make a user a member of a group, highlight the desired group in the "Not member of" list box. Then click the Add command button. The group now appears in the "Member of" list box.

To remove a user from a group, highlight the group in the "Member of" list box. Then click the Remove command button. The group no longer appears in the "Member of" list box.

You can make any number of group membership changes in this dialog box, but you must click OK when you are finished to make the changes effective.

On Windows NT Server domain controllers, there is an option in the Group Memberships dialog box to set a primary group for a user account. The primary group setting concerns file ownership and permissions, and only affects users of Macintosh computers who access files on a Windows NT Server computer and users of Windows NT computers who run POSIX-compliant applications. The default primary group setting is Domain Users. However, you can assign any global group as a user's primary group. In most Windows NT networks, you can simply accept the default setting for this option.

Profile

The Profile command button in the User Properties dialog box is used to configure the user's environment. You can configure the user profile path, logon script name, and home directory location.

When you click the Profile command button in the User Properties dialog box, the User Environment Profile dialog box appears. Figure 7-5 shows the User Environment Profile dialog box for Administrator.

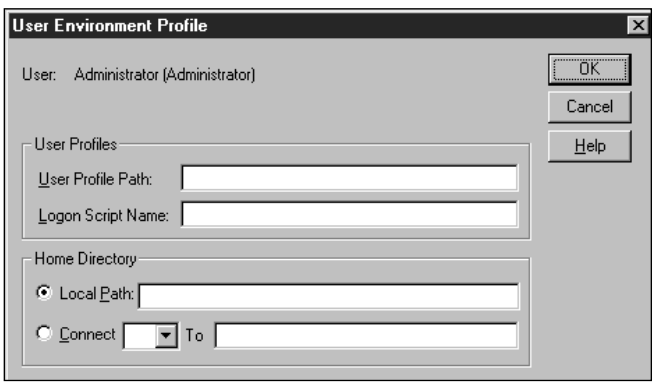


FIGURE 7-5 Administrator's environment profile

The user profile path is used to assign a location for the user's profile. 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 `<winntroot>\Profiles\%USERNAME%` folder. User profile paths must include the complete path to the folder that contains the user's profile, in the for-

mat of *Server_name**Share_name**Folder**Subfolder*. If no path is entered in the User Profile Path text box, Windows NT uses the default location.

Profiles and logon scripts are covered in more detail in Chapter 9.

The Logon Script Name text box is an optional configuration that enables you to enter the user's logon script filename, if the user has one. *Logon scripts* are batch files that run on a user's computer during the logon process. Many Windows NT installations don't use logon scripts. If you choose to use logon scripts, enter the user's logon script filename in the Logon Script Name text box. You should place a copy of each user's logon script file in the `Netlogon` share on every domain controller in the domain, or use directory replication to replicate the logon script file. Directory replication is covered in detail in Chapter 4.

The Home Directory section of the User Environment Profile dialog box is used to configure either a local home directory on the user's computer, or a server-based home directory.

A *home directory* (either local or server-based) is a user's default directory for the Save As and File Open dialog boxes in most Windows-based applications. Using server-based home directories enables the network administrator to easily backup user-created data files, because the user-created files are stored by default on the server instead of on individual computers. For security reasons, I recommend you place sever-based home directories on an NTFS partition.

If you select the radio button next to Local Path, you can enter the user's home directory in the format of *Drive_Letter:**Folder**Subfolder*. This assigns a user's home directory to a folder on the user's local computer.

If you want to use a server-based home directory, select the radio button next to Connect. Then select a drive letter to use for the user's home directory. The default drive letter is Z:. Next type a complete path in the form of *Server_name**Share_name**Folder**Subfolder* in the To text box. If the last folder in the path you type in this box does not yet exist, Windows NT will create it.

The most common way of assigning a server-based home directory is to first create a shared folder named `Users` on the server, and then to assign the path *Server_name*\Users\%USERNAME% as each user's home directory location. When the `%USERNAME%` variable is used in a path, Windows NT creates a home directory/folder (that is named using the user's account name) in the `Users` shared folder. Using this variable can simplify administration when creating a large number of user accounts because you can enter the same path for each new user, and Windows NT creates a unique home directory/folder for each user account.

Hours

The Hours command button in the User Properties dialog box is used to configure the hours that a user is allowed to log on. This command button is only available when managing Windows NT Server computers that are configured as domain controllers.

The logon hours configuration only affects the user's ability to access the domain controller—it does not affect a user's ability to log on to a Windows NT Workstation computer or other non-domain controller.

When you click the Hours command button in the User Properties dialog box, the Logon Hours dialog box appears. Figure 7-6 shows the Logon Hours dialog box for Administrator. Notice that by default all hours are available for logon. This is the default for all users, not just Administrator.

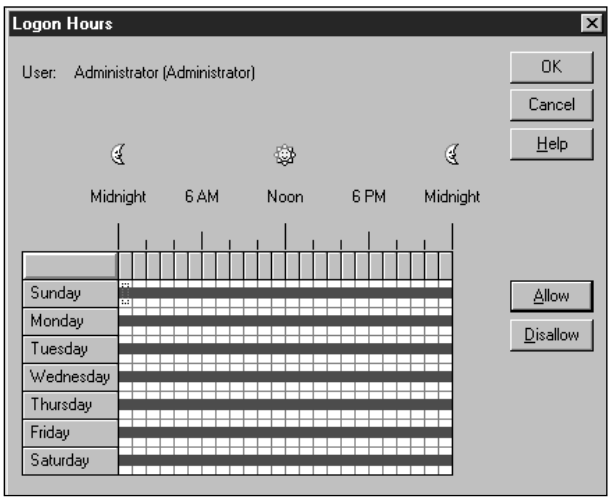


FIGURE 7-6 Administrator's logon hours

To modify the user's logon hours, use your mouse to highlight the hours you do *not* want the user to be able to log on, and click the Disallow command button. Or, you can use your mouse to highlight the entire graph, click the Disallow command button, then highlight the hours you *want* the user to be able to log on, and then click the Allow command button.

Figure 7-7 shows modified logon hours for a user named BillT. Notice that BillT can't log on between the hours of midnight and 3:00 a.m. The administrator

of BillT's network normally runs a tape backup during these hours, and does not want users to log on and open files (which may not be backed up) during the backup process.

Restricting a user's logon hours does not disconnect a user from a domain controller when the user's logon hours expire. A logon hours restriction only *prevents* a user from logging on to the domain controller during certain specified hours. If you want to forcibly disconnect users when their logon hours expire, additional steps must be taken.

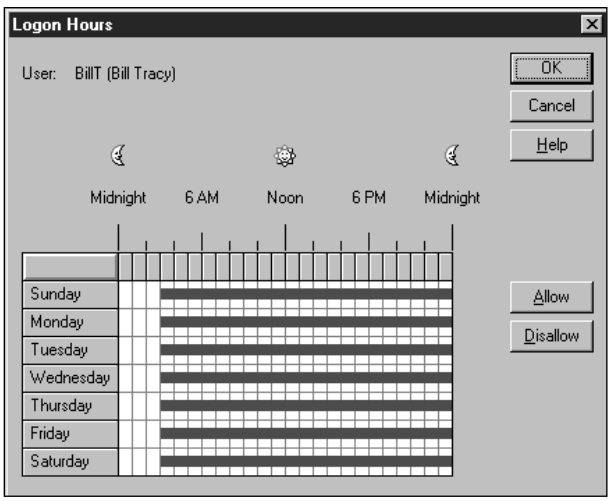


FIGURE 7-7 **User's logon hours restricted**

TO FORCIBLY DISCONNECT ALL USERS FROM THE DOMAIN CONTROLLER(S) WHEN THEIR LOGON HOURS EXPIRE, FOLLOW THESE STEPS:

1. Select Start ➪ Programs ➪ Administrative Tools (Common) ➪ User Manager for Domains.
2. Select Policies ➪ Account in the User Manager dialog box.
3. The Account Policy dialog box appears. Select the check box next to "Forcibly disconnect remote users from server when logon hours expire." Click OK.

Figure 7-8 shows the Account Policy dialog box. Notice that the check box next to "Forcibly disconnect remote users from server when logon hours expire" is selected. All settings in the Account Policy dialog box apply to all user accounts in the domain—no individual configurations are possible.

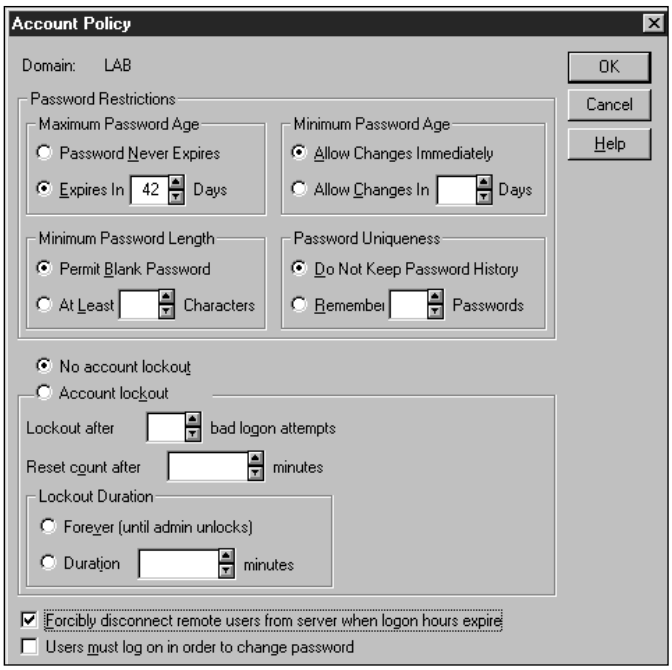


FIGURE 7-8 **Disconnecting users from the domain controller when logon hours expire**

Logon To

The Logon To command button in the User Properties dialog box is used to configure the names of computers from which a user can log on to the domain. This command button is only available on Windows NT Server computers that are configured as domain controllers.

When you click the Logon To command button in the User Properties dialog box, the Logon Workstations dialog box appears. Figure 7-9 shows the Logon Workstations dialog box for Administrator. Notice that by default a user may log on to any workstation (computer) on the network. This is the default setting for all users, not just Administrator.

If you want to limit the workstations to which a user can log on, select the radio button next to User May Log On To These Workstations, and then enter the computer name for up to eight workstations. The user will only be able to log on to the domain from the computers entered in this dialog box. Click OK.

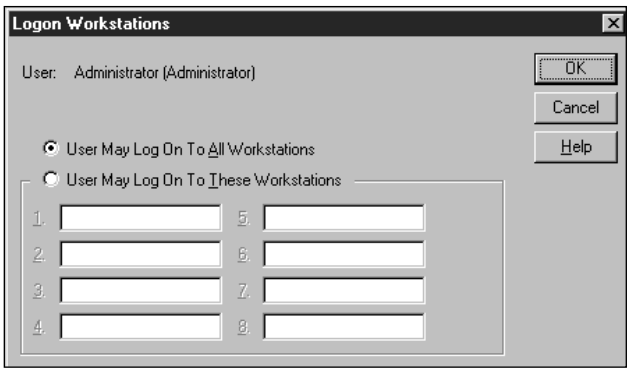


FIGURE 7-9 Configuring logon workstations

Account

The Account command button in the User Properties dialog box is used to configure account expiration and user account type. This command button is only available on Windows NT Server computers that are configured as domain controllers.

When you click the Account command button in the User Properties dialog box, the Account Information dialog box appears. Figure 7-10 shows the Account Information dialog box for Administrator. Notice that by default a user account never expires. This is the default setting for all users, not just Administrator.

FIGURE 7-10 Configuring account information

You might want to configure a user account expiration date for an employee working on a temporary or short-term basis. To set an account expiration, select the radio button next to "End of," and then enter the date you want the user's account to expire. Click OK. The user will not be forcibly disconnected from the domain controller when the account expires, but will not be able to log on after the account expiration date. You can't set an account expiration date on the two built-in user accounts, Administrator and Guest.

There are two options for account type: *global account* and *local account*. By default, all user accounts are configured as global accounts. A global account is designed for regular user accounts in this domain. Users can log on to the domain using a global account. Most Windows NT installations only use global accounts.

A local account is designed to enable users from untrusted domains to access resources on the domain controller(s) in this domain. Users can't log on using a local account. (Trust relationships are covered in detail in Chapter 10.)

Dialin

The Dialin command button in the User Properties dialog box is used to configure dialin permission for a user account. The dialin permission allows a user to log on by using a Dial-Up Networking connection.

When you click the Dialin command button in the User Properties dialog box, the Dialin Information dialog box, which is shown in Figure 7-11, appears. Notice that by default a user account is not granted the dialin permission.

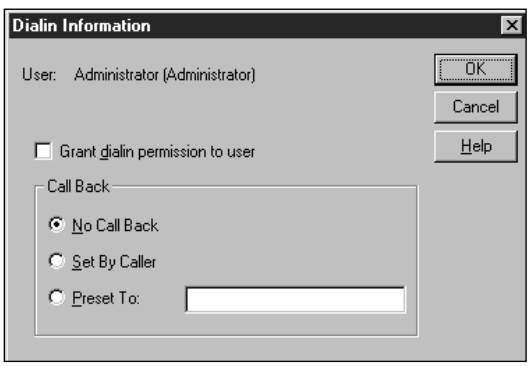


FIGURE 7-11 **Granting dialin permission to a user account**

The dialin permission should be granted to every user that needs access to the network by using a Dial-Up Networking connection. For example, traveling sales representatives need to access e-mail and other network resources from their

laptop computers, and employees who occasionally work from home may need to be able to dial in to access network resources from their home computers.

To grant a user the dialin permission, select the check box next to Grant dialin permission to user.

There are three options in the Call Back section: No Call Back, Set By Caller, and Preset To. The default setting is No Call Back.

If you select No Call Back, the user can dial in to the server, but the user can't request that the server break the connection and call the user back. Selecting No Call Back ensures that the user dialing in — not the server — is billed for any long distance telephone charges.

If you select Set By Caller, the server prompts the user for a telephone number. The server breaks the connection and calls the user back using this number, and thus the server incurs the bulk of any long distance telephone charges.

If you select Preset To, you must enter a telephone number that the server will always use to call back this user when the user dials in. This setting reduces the risk of unauthorized access to network resources, because the server always calls a preset telephone number, such as a user's home telephone number. An unauthorized user might be able to dial in and guess a password, but will not be able to direct the server to call back at any other number than the number specified in Preset To, and thus will not be able to connect to the network.

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 that are similar to the desired properties for the new user account, or
- 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.

For example, suppose that you want to create a user account to be used by an employee to 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 are copied to the new user account, with the exception of user name, full name, password, the account disabled option, and user rights and permissions.

To copy the Administrator user account, highlight Administrator in the Username list box in the User Manager dialog box. Select User ➢ Copy, and then type in a new user name and password for the new user account. Make any other desired changes in the User Properties dialog box, then click the Add command button. Then click Close. The newly created user has the same account properties as Administrator.

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. 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, select User ➢ New User in the User Manager dialog box. 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 group memberships, profile, logon hours, and so on to match the requirements of the user accounts you will create using this template. When you create a user account to be used as a template, I recommend that you select the Account Disabled check box so that no one can log on using this account.

Figure 7-12 shows the User Properties dialog box of a user account that is designed to be used as a template. Note that the Account Disabled check box is selected.

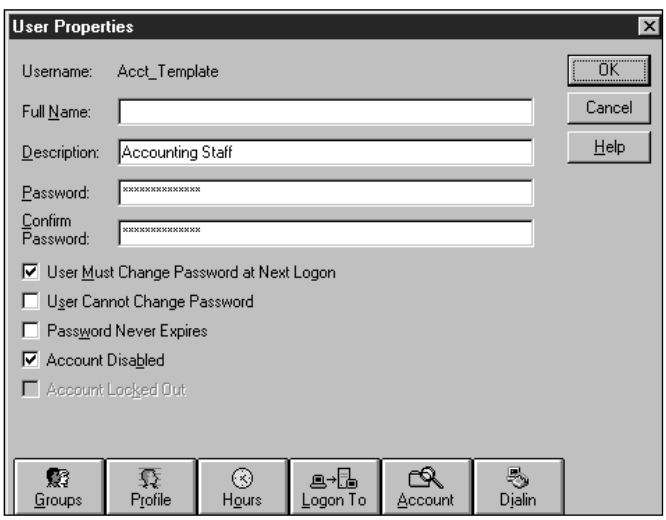


FIGURE 7-12 Configuring a user account to be used as a template

To use a template, highlight the template user account in the User Manager dialog box, then select User ➪ Copy. Then type in a new user name and password for the new user account. Make any other desired changes in the User Properties dialog box, then click the Add command button. Then click Close.

All properties of the template user account are copied to the new user account, with the exception of user name, full name, password, the account disabled option, and user rights and permissions.

Applying Properties to Multiple Accounts

Occasionally you might want to apply a property to multiple user accounts.

For example, suppose that you recently installed the *Remote Access Service* (RAS) on one of your network servers, and now you want to grant several users the dialin permission so they can connect to the network from their computers at home.

Another situation where you might want to apply properties to multiple user accounts is right after you create several new user accounts. You can create several bare-bones user accounts, consisting only of user names, full names, and passwords. Then you can select all of the new user accounts, and configure them all at once with identical properties. You can use this method as an alternative to using a user account as a template.

TO APPLY A PROPERTY (OR PROPERTIES) TO MULTIPLE USER ACCOUNTS, FOLLOW THESE STEPS:

1. Highlight the first user account you want to apply a property to in the User Manager dialog box. Then press and hold Ctrl while you click each additional user account that you want to apply that property to. Then select User ➪ Properties.
2. The User Properties dialog box appears. The users you selected in Step 1 are listed in the Users list box. Figure 7-13 shows the User Properties dialog box. Notice that multiple users are displayed in the Users list box.
3. Configure the user account property (or properties) as desired. All changes made will apply to all of the users in the Users list box. Then click OK.

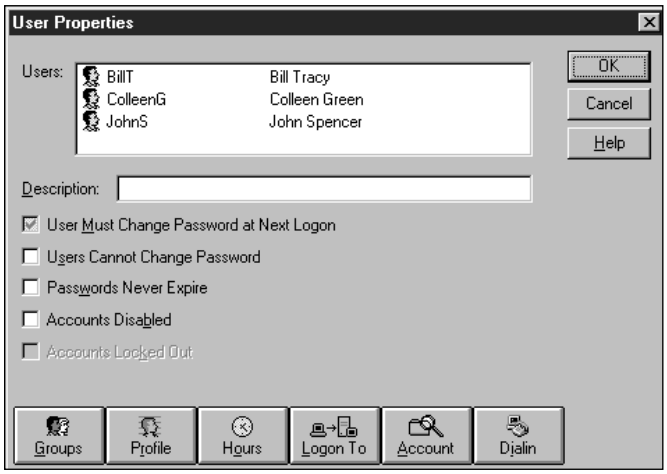


FIGURE 7-13 **Selecting multiple user accounts**

Renaming and Deleting User Accounts

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

Renaming a user account retains all of the account properties, including group memberships, permissions, and rights for the new user of the account. You might want to rename a user account when a new staff member replaces an employee who has left the company.

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

The two built-in accounts, Administrator and Guest, can't be deleted, although they can be renamed. The following section details how to rename and delete a user accout.

TO RENAME A USER ACCOUNT, FOLLOW THESE STEPS:

1. Select Start ➪ Programs ➪ Administrative Tools (Common) ➪ User Manager (or User Manager for Domains).
2. In the User Manager dialog box, highlight the user account that you want to rename. Select User ➪ Rename.
3. Type in the new user name for the user account in the Rename dialog box. Click OK.
4. Double-click the renamed user account in the User Manager dialog box.
5. The User Properties dialog box appears. Assign (and confirm) a new password to the renamed user account. Select the check box next to User Must Change Password at Next Logon. Click OK.
6. Exit User Manager (or User Manager for Domains).
7. If the renamed user account has an associated home directory, also rename the home directory using Windows NT Explorer.

TO DELETE A USER ACCOUNT, FOLLOW THESE STEPS:

1. Select Start ➪ Programs ➪ Administrative Tools (Common) ➪ User Manager (or User Manager for Domains).
2. In the User Manager dialog box, highlight the user account you want to delete. Press Delete.
3. A warning message appears. Click OK to continue.
4. Another warning dialog box appears. Click Yes to delete the user account. The user account is deleted.
5. Exit User Manager (or User Manager for Domains).

Creating and Managing Groups

The remainder of this chapter is dedicated to groups. Using groups is a convenient and efficient way to assign rights and permissions to multiple users.

Groups are collections of user accounts. There are four types of groups in Windows NT: *local groups, global groups, built-in groups,* and *special groups.*

Local Groups

Local groups are primarily used to control access to resources. In a typical Windows NT configuration, a local group is assigned permissions to a specific resource, such as a shared folder or a shared printer. Individual user accounts and global groups (discussed later in this chapter) are made members of this local group. The result is that all members of the local group now have permissions to the resource. 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.

In Windows NT, all domain controllers (within a single domain) maintain identical copies of the same directory database, while each non-domain controller maintains its own separate directory database. All user accounts and group accounts are stored in the directory database in which they are created. For example, if you create a local group in the LAB domain, it is stored in the LAB domain directory database. If you create a local group on a Windows NT Workstation computer, it is stored in the NT Workstation computer's local directory database.

Local groups can be created on any Windows NT computer. A local group in the directory database on a domain controller can be assigned permissions to resources on any domain controller in the domain. However, a local group in the directory database on a domain controller cannot be assigned permissions to resources on any non-domain controller. (Remember that non-domain controllers include stand-alone servers, member servers, and all Windows NT Workstation computers.) A local group in the directory database on a non-domain controller can be assigned permissions to resources only on that computer.

A local group can contain various user accounts and global groups, depending on whether the local group is located in the directory database on a domain controller, on a non-domain controller that is a member of a domain, or on a non-domain controller that is not a member of a domain.

A local group in the directory database on a domain controller can contain individual user accounts and global groups from the domain directory database, and can also contain user accounts and global groups from the directory database of any trusted domain. A *trusted domain* is a domain whose users can access resources in the domain that "trusts" it. Trust relationships are covered in more detail in Chapter 10.

A local group in the directory database on a non-domain controller that is a member of a domain (such as a member server or a Windows NT Workstation

computer that is a member of the domain) can contain individual user accounts from the local directory database, user accounts and global groups from the directory database of the member domain, and user accounts and global groups from the directory database of any trusted domain.

A local group in the directory database on a non-domain controller that is *not* a member of a domain (such as a stand-alone server or a Windows NT Workstation computer that is a member of a workgroup) can only contain individual user accounts from the local directory database.

Local groups can't contain other local groups.

The next section explains how local groups are created.

TO CREATE A NEW LOCAL GROUP, FOLLOW THESE STEPS:

1. Select Start ➪ Programs ➪ Administrative Tools (Common) ➪ User Manager (or User Manager for Domains).
2. Highlight any of the groups listed in the Groups list box. (The reason for this is the first user in the Username list box is highlighted by default, and if this user is not unhighlighted, the user will automatically become a member of the new local group you create.) Select User ➪ New Local Group.
3. The New Local Group dialog box appears. In the Group Name text box, type in a name for the new local group. In the Description text box, type a description if you want—such as the name of the resource the group will have permissions to. This text box is optional. Click the Add command button.
4. The Add Users and Groups dialog box appears. Highlight the user accounts and/or global groups from the Names list box that you want to make members of the new local group. Then click the Add command button. The names you selected appear in the Add Names list box. Click OK.
5. The New Local Group dialog box reappears. Figure 7-14 shows the New Local Group dialog box. Notice that several user accounts and one global group are listed as members of the new local group. Also note that the description reflects the resource to which the new local group has permissions. Click OK.
6. The User Manager dialog box reappears. The new local group appears in the Groups list box. Exit User Manager (or User Manager for Domains).

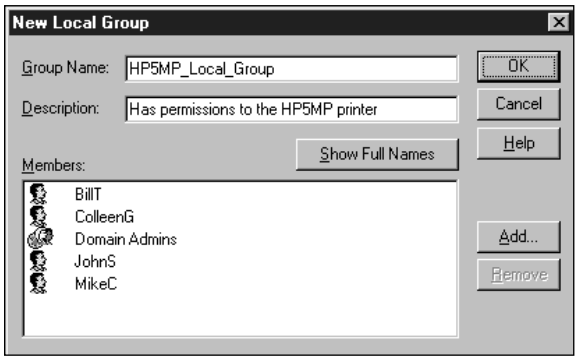


FIGURE 7-14 **Creating a new local group**

Global Groups

Global groups are primarily used to organize users that perform similar tasks or have similar network access requirements. In a typical Windows NT configuration, user accounts are placed in a global group, the global group is made a member of one or more local groups, and each local group is assigned permissions to a resource. The advantage of using global groups is ease of administration — the network administrator can manage large numbers of users by placing them in global groups.

Suppose when the 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 member server. The administrator creates a new local group on the member server and assigns the new local group permissions to the shared printer. Then the administrator selects, from the domain directory database, the global groups that contain the user accounts that need access to the shared printer. The administrator makes these global groups members of the new local group on the member server. The result is that all domain user accounts that are members of the selected global groups now have access to the shared printer.

A global group can only be created on a domain controller, and can only contain individual user accounts from the domain directory database that contains

the global group. Global groups can't contain local groups, other global groups, or user accounts from other domains.

Although it is not a preferred practice, you can assign rights and permissions to global groups. Global groups can be assigned permissions to shared files and folders on domain controllers, member servers, NT Workstation computers that are members of the domain, and computers from trusted domains.

Creating a new global group

The following section explains how to create a new global group.

TO CREATE A NEW GLOBAL GROUP, FOLLOW THESE STEPS:

1. Select Start ≥ Programs ≥ Administrative Tools (Common) ≥ User Manager for Domains.
2. Highlight any of the groups listed in the Groups list box. (The reason for this is that the first user in the Username list box is highlighted by default, and if this user is not unhighlighted, the user will automatically become a member of the new global group you create.) Select User ≥ New Global Group.
3. The New Global Group dialog box appears. In the Group Name text box, type in a name for the new global group. In the Description text box, type a description of the group. This text box is optional. Highlight the user accounts from the Not Members list box that you want to make members of the new global group. Then click the Add command button. The names you selected appear in the Members list box. Figure 7-15 shows the New Global Group dialog box. Notice that two user accounts are listed as members of the new global group. Click OK.

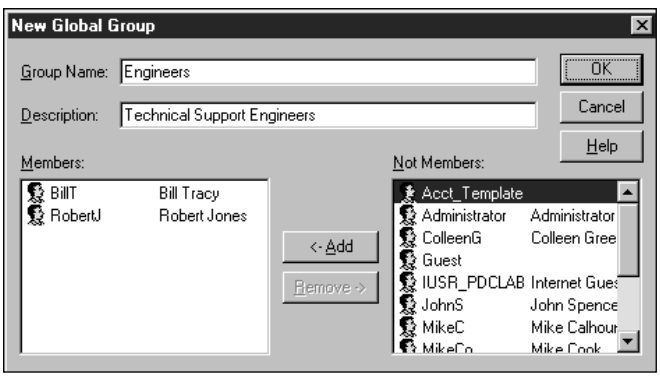


FIGURE 7-15 **Creating a new global group**

4. The User Manager dialog box reappears. The new global group appears in the Groups list box. Exit User Manager for Domains.

Comparison of Local and Global Groups

Local and global groups are complex topics that can be confusing.

exam preparation pointer 

Local and global groups are integral parts of many objectives on the three Windows NT 4.0 Microsoft Certified Professional exams. You must know the characteristics and uses of local and global groups—and know them cold—in order to pass the exams—especially the Enterprise exam.

To help simplify the important information about each type of group, I've prepared a comparison table for you. Table 7-2 summarizes the basic characteristics of local and global groups. Remember that the table is only a summary—you should refer to the detailed descriptions of local and global groups in the previous sections for complete coverage of these topics.

TABLE 7-2 COMPARISON OF LOCAL AND GLOBAL GROUPS

CHARACTERISTIC	*LOCAL GROUPS*	*GLOBAL GROUPS*
Primary purpose/use	Used to control access to network resources.	Used to organize users that perform similar tasks or have similar network access requirements.
Where created	On any Windows NT computer.	Only on a domain controller.
Can contain	User accounts and global groups. (The specific user accounts and global groups that can be contained in a local group depend on the type of computer on which the directory services database that contains the local group in question is located.)	User accounts from the domain directory database that contains the global group.

continued

TABLE 7-2 *(continued)*

CHARACTERISTIC	LOCAL GROUPS	GLOBAL GROUPS
Can't contain	Other local groups.	Local groups, other global groups, or user accounts from other domains.
Can be assigned permissions to	Resources on any domain controller in the domain, if the local group is created on a domain controller; otherwise, only resources on the local computer.	Not a preferred practice, but can be assigned permissions to a resource on any computer in the domain, or on any computer in any trusted domain.

Built-in Groups

Built-in groups are groups with preset characteristics that are automatically created during the installation of Windows NT. The actual built-in groups created during installation depend on whether the computer is configured as a domain controller or a non-domain controller.

The members of built-in local groups have the rights and/or permissions to perform certain administrative tasks. You can assign users to the built-in local groups that most closely match the tasks that the users need to perform. If there isn't a built-in local group that has the rights and/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 and/or permissions to accomplish the task or access the resource.

You can use built-in global groups to organize the user accounts in your domain. As you recall from the previous section, you can also create additional global groups to further organize your domain's user accounts by task or network access requirements.

You can assign permissions to and remove permissions from built-in groups. (An exception is the built-in Administrators group — this group always has full rights and permissions to administer the computer or domain.) You can also assign users to and remove users from built-in groups. Built-in groups can't be renamed or deleted.

The following tables list the various built-in groups on Windows NT domain controllers and non-domain controllers, and give a brief description of each group's purpose or function. The table of built-in groups on domain controllers

indicates whether each built-in group is a local or global group. The table of built-in groups on non-domain controllers contains only local groups.

Table 7-3 lists the built-in groups on domain controllers, and Table 7-4 lists the built-in groups on non-domain controllers.

TABLE 7-3 BUILT-IN GROUPS ON DOMAIN CONTROLLERS

BUILT-IN GROUP NAME	*TYPE OF GROUP*	*DESCRIPTION*
Administrators	Local	Has full administrative rights and permissions to administer the domain; initially contains the Domain Admins global group.
Backup Operators	Local	Has permissions to back up and restore files and folders on all domain controllers in the domain.
Guests	Local	Has no initial permissions; initially contains the Domain Guests global group.
Replicator	Local	Used by the Windows NT Directory Replicator service.
Users	Local	Has no initial permissions; initially contains the Domain Users global group.
Account Operators	Local	Can create, delete, and modify user accounts, local groups, and global groups, with the exception of Administrators and Server Operators groups.
Printer Operators	Local	Can create and manage printers on any domain controller in the domain.
Server Operators	Local	Has permissions to back up and restore files and folders on all domain controllers in the domain; can share folders on any domain controller in the domain.
Domain Admins	Global	No initial permissions; initially contains the built-in Administrator user account.
Domain Users	Global	No initial permissions; initially contains the built-in Administrator user account; when new user accounts are created, they are automatically made members of this group.
Domain Guests	Global	No initial permissions; initially contains the built-in Guest user account.

TABLE 7-4 BUILT-IN LOCAL GROUPS ON NON-DOMAIN CONTROLLERS

BUILT-IN LOCAL GROUP NAME	*DESCRIPTION*
Administrators	Has full administrative rights and permissions to administer the computer; initially contains the built-in Administrator user account.
Backup Operators	Has permissions to back up and restore files and folders on the computer.
Guests	Has no initial permissions; initially contains the built-in Guest user account.
Replicator	Used by the Windows NT Directory Replicator service.
Users	Has no initial permissions; when new user accounts are created, they are automatically made members of this group.
Power Users	Can create and modify user and group accounts, with the exception of the Administrator user account and the Administrators group; can share folders and printers.

Special Groups

Special groups are created by Windows NT and are used for specific purposes by the operating system.

These groups don't appear in User Manager or User Manager for Domains. Special groups are only visible in Windows NT utilities that assign permissions to network resources, such as a printer's Properties dialog box, and Windows NT Explorer.

You can assign permissions to and remove permissions from special groups. You can't assign users to special groups, and you can't rename or delete these groups. Special groups are sometimes called system groups.

There are five special groups: *Everyone*, *Interactive*, *Network*, *System*, and *Creator Owner*.

Any user who accesses a Windows NT 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 unauthorized users who accidentally or intentionally breach your system security. If your computer is connected to the Internet, over-the-network also means over-the-Internet. Everyone means *everyone*. You should consider limiting the permissions assigned to the Everyone group to those that you really want everyone to have.

Any user who physically sits at a computer and logs on locally to a Windows NT computer is a member of the Interactive special group. If you want to assign permissions to a resource that is limited to users who have physical access to a computer, consider assigning these permissions to the Interactive group. You are only a member of the Interactive group during the time that you are logged on locally.

Any user who accesses resources on a Windows NT computer over-the-network is a member of the Network special group. If you want to assign permissions to a resource that is limited to users who access the computer over-the-network, consider assigning these permissions to the Network group. You are only a member of the Network group during the time that you access resources on a computer over-the-network.

The System special group is used by the Windows NT operating system. The System special group is not normally assigned any permissions to network resources.

A user who creates a file, folder, or a print job is considered a member of the Creator Owner special group for that object. 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.

Renaming and Deleting Groups

I apologize if you envisioned a time-saving solution when you read the above heading, but unfortunately, the fact of the matter is, you can't rename groups. You can delete user-created groups, but you can't delete built-in or special groups. Deleting a group does not delete the user accounts that the group contains.

TO DELETE A GROUP, FOLLOW THESE STEPS:

1. Select Start ➪ Programs ➪ Administrative Tools (Common) ➪ User Manager (or User Manager for Domains).
2. In the User Manager dialog box, highlight the group you want to delete. Press Delete.

3. A warning message appears. Click OK to continue.
4. Another warning message is displayed. Click the Yes command button to delete the group.
5. The group is deleted. Exit User Manager (or User Manager for Domains).

Key Point Summary

This chapter explored and outlined the properties, creation, and management of user accounts and groups.

- *User accounts* are records that contain unique user information, and enable users to log on to Windows NT. There are two kinds of user accounts: built-in user accounts, and the user accounts that you create. The two built-in user accounts are Administrator and Guest. You can create user accounts by using User Manager (on a Windows NT Workstation computer) or User Manager for Domains (on a Windows NT Server computer). User account names can be up to twenty characters in length, must be unique within the domain, can't be the same as a group name within the domain (or non-domain controller), and may not contain certain special characters. Often a naming convention for user accounts is adopted, along with a way to handle exceptions that would result in two user names being identical. Using passwords protects the security of the network. Normally, users choose their own passwords, although in some high security situations the network administrator may maintain user passwords. Common sense security measures should be taken by users to protect their passwords.
- User accounts have numerous options, called *user account properties,* that can be configured, including: group membership, profile, logon scripts, logon hours, workstation logon restrictions, account expiration, and dialin permission. These properties are configured in the User Properties dialog box in User Manager or User Manager for Domains.
  - The *Groups* command button in the User Properties dialog box is used to configure which group(s) a user is a member of.

- The *Profile* command button in the User Properties dialog box is used to configure the user's environment, including user profile path, logon script name, and home directory location. The variable %USERNAME% is often used when assigning a server-based home directory to many users, because using the variable enables you to enter the same path for multiple users, and yet results in each user having a unique home directory based on their unique user account name.
- The *Hours* command button in the User Properties dialog box is used to configure the hours that a user can log on.
- The *Logon To* command button in the User Properties dialog box is used to configure the names of computers from which a user can log on to the domain.
- The *Account* command button in the User Properties dialog box is used to configure account expiration and user account type. You might want to configure a user account expiration date for a temporary employee. You can't set an account expiration date on the two built-in accounts, Administrator and Guest.
- The *Dialin* command button in the User Properties dialog box is used to configure the dialin permission for a user account. This permission enables a user to log on using a Dial-Up Networking connection. There are three options in the Call Back section: No Call Back (the default setting), Set By Caller, and Preset To.
- The Hours, Logon To, and Account command buttons are only available on Windows NT Server computers that are configured as domain controllers.

- User accounts can be copied using User Manager or User Manager for Domains. You can copy an existing user account that has properties similar to the properties you want the new user account to have, or 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.
- You can also use User Manager or User Manager for Domains to apply a property (or properties) to multiple user accounts at the same time. User accounts can also be renamed and deleted, with the exception of the two built-in accounts, Administrator and Guest.
- Using groups is a convenient and efficient way to assign rights and permissions to multiple users.

- *Local groups* are primarily used to control access to resources. Typically, a local group is assigned permission to a specific resource (such as a shared folder or shared printer), and then user accounts and global groups are made members of the local group. As a result, all members of the local group have permission to the resource. Local groups can contain individual user accounts and global groups. (The specific user accounts and global groups that can be contained in a local group depend on the type of computer that the directory services database is located on that contains the local group in question.) Local groups can't contain other local groups. Local groups can be assigned permissions to resources on any domain controller in the domain (if the local group is created on a domain controller); otherwise, local groups can be assigned permissions only to resources on the local computer. Local groups can be created on any Windows NT computer.
- *Global groups* are primarily used to organize users who perform similar tasks or have similar network access requirements. Global groups can contain user accounts from the domain directory database that contains the global group; but global groups can't contain local groups, other global groups, or user accounts from other domains. A global group can only be created on a domain controller.
- There are a number of built-in local and global groups that are automatically created during the installation of Windows NT. Built-in local groups can be used to assign users rights and/or permissions to perform certain administrative tasks. Built-in global groups are used to organize the user accounts in a domain. The actual built-in groups present on a Windows NT computer depend on whether the computer is configured as a domain controller or a non-domain controller. The built-in local groups on domain controllers are: Administrators, Backup Operators, Guests, Replicator, Users, Account Operators, Printer Operators, and Server Operators. The built-in global groups on domain controllers are: Domain Admins, Domain Users, and Domain Guests. The built-in groups on non-domain controllers are: Administrators, Backup Operators, Guests, Replicator, Users, and Power Users. All the built-in groups on non-domain controllers are local groups.

- There are five *special groups* (sometimes called *system groups*) created by Windows NT: Everyone, Interactive, Network, System, and Creator Owner.

You can assign permissions to and remove permissions from special groups, but you can't assign users to special groups.

- You can't rename groups. You can delete user-created groups by using User Manager or User Manager for Domains, but you can't delete built-in or special groups.

Applying What You've Learned

Now it's time to regroup, review, and apply what you've learned in this chapter.

The questions in the following Instant Assessment section bring to mind key facts and concepts.

The hands-on lab exercise will really reinforce what you've learned, and give you an opportunity to practice some of the tasks tested by the Microsoft Certified Professional exams.

Instant Assessment

1. What are the two built-in user accounts?
2. What Windows NT tool can you use to create user accounts?
3. Name two common user account naming conventions.
4. Which groups can be deleted? Which groups can't be deleted?
5. What are the six command buttons in the User Properties dialog box in User Manager for Domains that can be used to configure various user account properties?
6. What variable is often used when assigning a server-based home directory to many users?
7. Suppose that you wanted to create several new user accounts that all had identical properties. What could you do to accomplish this in an efficient manner?
8. What is the primary purpose of local groups? What is the primary purpose of global groups?

9. Where can local groups be created? Where can global groups be created?
10. Suppose that you want to use groups to assign permissions to a shared folder on your network. How could you accomplish this?
11. List the eight built-in local groups on domain controllers and the three built-in global groups on domain controllers.
12. List the six built-in local groups on non-domain controllers.
13. What are the five special groups in Windows NT?
14. Why is it important to limit the permissions assigned to the Everyone group, especially if your computer is connected to the Internet?
15. Which groups can be renamed?

T/F

16. You should pick a name that is familiar to you, such as your own name, or the name of a family member or pet, to use as your password. ____

For answers to the Instant Assessment questions see Appendix D.

Hands-on Lab Exercise

The following hands-on lab exercise provides you with a practical opportunity to apply the knowledge you've gained in this chapter about managing user and group accounts.

Lab 7.10 *Creating and managing user and group accounts*

Workstation
Server
Enterprise

The purpose of this lab is to give you hands-on experience creating user accounts, assigning home directories, managing user account properties, creating group accounts, and assigning user accounts to groups. You will also create user account templates to help simplify the creation of user accounts.

This lab consists of four parts:

Part 1: Creating the `Users` folder

Part 2: Creating group accounts

Part 3: Creating user account templates

Part 4: Creating and managing user accounts

In this lab you'll create users and groups for the local office of a sales organization. Within this organization there are several employees. Table 7-5 shows the organization's employees and their job titles.

TABLE 7-5 SALES ORGANIZATION EMPLOYEES

EMPLOYEE	*JOB TITLE*
Pam Rhodes	District Manager
John Spencer	Sales Manager
Robert Jones	Accounting Manager
Colleen Green	Sales Representative
Bill Tracy	Sales Representative
Mike Calhoun	Sales Representative
Nancy Yates	Accounting Staff
Mike Cook	Accounting Staff

The users will select their own passwords when they first access their user accounts. Each user will have a home folder on the primary domain controller named PDCLAB.

Begin this lab by booting your computer to Windows NT Server. Log on as Administrator. (Remember, the password is *password*.)

Follow the steps below carefully.

Part 1: Creating the `Users` folder

In this section you create and share a `Users` folder in Windows NT Explorer. The `Users` folder will eventually contain a home directory for each user account.

1. Select Start ≥ Programs ≥ Windows NT Explorer.
2. In the All Folders list box, highlight the drive on which your NTFS partition is located. (This is probably drive D:.) Select File ≥ New ≥ Folder.
3. A folder named `New Folder` is created and appears in the "Contents of D:." Edit the folder's name so that it is called **Users**. Press Enter.
4. Highlight the `Users` folder in the Windows NT Explorer dialog box. Select File ≥ Sharing.
5. In the Users Properties dialog box, select the radio button next to Shared As. Accept the default Share Name of Users. Click OK.
6. Exit Windows NT Explorer. Continue to Part 2.

Part 2: Creating group accounts

In this section you create three new global groups: Managers, Sales, and Accounting.

1. Select Start ➪ Programs ➪ Administrative Tools (Common) ➪ User Manager for Domains.
2. Highlight any of the groups listed in the Groups list box. (The reason for this is that the first user in the Username list box is highlighted by default, and if this user is not unhighlighted, the user will automatically become a member of the new global group you create.) Select User ➪ New Global Group.
3. The New Global Group dialog box appears. In the Group Name text box, type in **Managers**. In the Description text box, type in **Managers of the Sales Organization**. Click OK.
4. The User Manager dialog box reappears. Select User ➪ New Global Group.
5. The New Global Group dialog box appears. In the Group Name text box, type in **Sales**. In the Description text box, type in **Sales Representatives**. Click OK.
6. The User Manager dialog box reappears. Select User ➪ New Global Group.
7. The New Global Group dialog box appears. In the Group Name text box, type in **Accounting**. In the Description text box, type in **Accounting Staff**. Click OK.
8. The User Manager dialog box reappears. You have now created three new global groups: Managers, Sales, and Accounting. Continue to Part 3.

Part 3: Creating user account templates

In this section you create two user account templates, one that will be used to create user accounts for sales representatives, and another that will be used to create user accounts for accounting staff.

1. In the User Manager dialog box, select User ➪ New User.
2. The New User dialog box appears. Type the bolded information below in the appropriate text boxes:
   - User Name: **Sales_User**
   - Full Name: (Leave this box blank.)
   - Description: **Sales Representative**
   - Password: **newuser**
   - Confirm Password: **newuser**

   Select the check box next to User Must Change Password at Next Logon. Select the check box next to Account Disabled. Click the Groups command button.

3. The Group Memberships dialog box appears. In the "Not member of" list box, highlight Sales. Click the Add command button. (Notice that the Sales group, along with Domain Users, is now listed in the "Member of" list box.) Click OK.
4. The New User dialog box reappears. Click the Dialin command button.
5. The Dialin Information dialog box appears. Select the check box next to "Grant dialin permission to user." Accept the default of No Call Back in the Call Back section. Click OK.
6. The New User dialog box reappears. Click the Profile command button.
7. The User Environment Profile dialog box appears. In the Home Directory section, select the radio button next to Connect. Accept the Z: in the drop-down list box. In the To text box, type: **\\PDCLAB\USERS\%USERNAME%**. Click OK.
8. The New User dialog box reappears. Click the Add command button.
9. The New User dialog box reappears. Type the following bolded information in the appropriate text boxes:
   - User Name: **Acct_User**
   - Full Name: (Leave this box blank.)
   - Description: **Accounting Staff**
   - Password: **newuser**
   - Confirm Password: **newuser**

   Select the check box next to User Must Change Password at Next Logon. Select the check box next to Account Disabled. Click the Groups command button.
10. The Group Memberships dialog box appears. In the "Not member of" list box, highlight Accounting. Click the Add command button. (Notice that the Accounting group, along with Domain Users, is now listed in the "Member of" list box.) Click OK.
11. The New User dialog box reappears. Click the Hours command button.
12. The Logon Hours dialog box appears. Using your mouse, highlight the entire graph. Click the Disallow command button. Using your mouse, highlight the area on the graph that represents 6:00 a.m. to 9:00 p.m. Monday through Friday. Click the Allow command button. Click OK.
13. The New User dialog box reappears. Click the Profile command button.
14. The User Environment Profile dialog box appears. In the Home Directory section, select the radio button next to Connect. Accept the Z: in the drop-down list box. In the To text box, type: **\\PDCLAB\USERS\ %USERNAME%**. Click OK.

15. The New User dialog box reappears. Click the Add command button. Click the Close command button. Notice that your two new user account templates, Sales_User and Acct_User, now appear in the Username list box within the User Manager dialog box. Continue to Part 4.

Part 4: Creating and managing user accounts

In this section you create user accounts from scratch and also use the user account templates to create user accounts. You assign some of the new user accounts to groups.

1. In the User Manager dialog box, select User➢New User.
2. The New User dialog box appears. Type the following bolded information in the appropriate text boxes:
   - User Name: **PamR**
   - Full Name: **Pam Rhodes**
   - Description: **District Manager**
   - Password: **newuser**
   - Confirm Password: **newuser**

   Select the check box next to User Must Change Password at Next Logon. Click the Groups command button.
3. The Group Memberships dialog box appears. In the "Not member of" list box, highlight Accounting. Then press and hold Ctrl while you scroll down and click Managers and Sales. Click the Add command button. (The Accounting, Managers, and Sales groups, along with Domain Users, should now be listed in the "Member of" list box.) Click OK.
4. The New User dialog box reappears. Click the Add command button.
5. The New User dialog box reappears. Type the following bolded information in the appropriate text boxes:
   - User Name: **JohnS**
   - Full Name: **John Spencer**
   - Description: **Sales Manager**
   - Password: **newuser**
   - Confirm Password: **newuser**

   Select the check box next to User Must Change Password at Next Logon. Click the Groups command button.
6. The Group Memberships dialog box appears. In the "Not member of" list box, highlight Managers. Then press and hold Ctrl while you click Sales.

Click the Add command button. (The Managers and Sales groups, along with Domain Users, should now be listed in the "Member of" list box.) Click OK.

7. The New User dialog box reappears. Click the Add command button.
8. The New User dialog box reappears. Type the following bolded information in the appropriate text boxes:
   - User Name: **RobertJ**
   - Full Name: **Robert Jones**
   - Description: **Accounting Manager**
   - Password: **newuser**
   - Confirm Password: **newuser**

   Select the check box next to User Must Change Password at Next Logon. Click the Groups command button.
9. The Group Memberships dialog box appears. In the "Not member of" list box, highlight Accounting. Then press and hold Ctrl while you scroll down and click Managers. Click the Add command button. (The Accounting and Managers groups, along with Domain Users, should now be listed in the "Member of" list box.) Click OK.
10. The New User dialog box reappears. Click the Add command button. Click the Close command button.
11. The User Manager dialog box reappears. Notice that the three users you just created are in the Username list box. Highlight JohnS, and then press and hold Ctrl while you click PamR and RobertJ. Select User ➢ Properties.
12. The User Properties dialog box appears. Notice the three users you selected are listed in the Users list box. Click the Dialin command button.
13. The Dialin Information dialog box appears. Select the check box next to "Grant dialin permission to user." Accept the default of No Call Back in the Call Back section. Click OK.
14. The User Properties dialog box reappears. Click the Profile command button.
15. The User Environment Profile dialog box appears. In the Home Directory section, select the radio button next to Connect. Accept the Z: in the drop-down list box. In the To text box, type: **\\PDCLAB\USERS\%USERNAME%**. Click OK.
16. The User Properties dialog box reappears. Click OK. You have now granted dialin permission and assigned home folders to JohnS, PamR, and RobertJ.
17. The User Manager dialog box reappears. Highlight Sales_User. Select User ➢ Copy.

18. The Copy of Sales_User dialog box appears. Type the following bolded information in the appropriate text boxes:
    - User Name: **ColleenG**
    - Full Name: **Colleen Green**
    - Description: (This is already filled in.)
    - Password: **newuser**
    - Confirm Password: **newuser**

    Select the check box next to User Must Change Password at Next Logon. Click Groups. Notice that the Sales group, as well as Domain Users, is listed in the "Member of" list box. Click OK.
19. In the Copy of Sales_User dialog box, click the Dialin command button. In the Dialin Information dialog box, notice that the check box next to "Grant dialin permission to user" is selected. Click OK.
20. In the Copy of Sales_User dialog box, click the Add command button.
21. The Copy of Sales_User dialog box reappears. Type the following bolded information in the appropriate text boxes:
    - User Name: **BillT**
    - Full Name: **Bill Tracy**
    - Description: (This is already filled in.)
    - Password: **newuser**
    - Confirm Password: **newuser**

    Select the check box next to User Must Change Password at Next Logon. Click the Add command button.
22. The Copy of Sales_User dialog box reappears. Type the bolded information below in the appropriate text boxes:
    - User Name: **MikeC**
    - Full Name: **Mike Calhoun**
    - Description: (This is already filled in.)
    - Password: **newuser**
    - Confirm Password: **newuser**

    Select the check box next to User Must Change Password at Next Logon. Click the Add command button. Click the Close command button.
23. The User Manager dialog box reappears. Notice that your new users now appear in the Username list box. Highlight the Acct_User. Select User ➪ Copy.

24. The Copy of Acct_User dialog box appears. Type the following bolded information in the appropriate text boxes:
    - User Name: **NancyY**
    - Full Name: **Nancy Yates**
    - Description: (This is already filled in.)
    - Password: **newuser**
    - Confirm Password: **newuser**

    Select the check box next to User Must Change Password at Next Logon. Click the Groups command button. Notice that the Accounting group, in addition to Domain Users, appears in the "Member of" list box. Click OK.
25. In the Copy of Acct_User dialog box, click the Hours command button. In the Logon Hours dialog box, notice that this user will be able to log on between 6:00 a.m. and 9:00 p.m. Monday through Friday. Click OK.
26. In the Copy of Acct_User dialog box, click the Add command button.
27. The Copy of Acct_User dialog box reappears. Type the following bolded information in the appropriate text boxes:
    - User Name: **MikeCo**
    - Full Name: **Mike Cook**
    - Description: (This is already filled in.)
    - Password: **newuser**
    - Confirm Password: **newuser**

    Select the check box next to User Must Change Password at Next Logon. Click the Add command button. Then click the Close command button.
28. The User Manager dialog box reappears. Notice that the new users you created appear in the Username list box. Exit User Manager.