

[\[Previous\]](#) [\[Next\]](#)

Chapter 10

Setting Up and Managing User Accounts

About This Chapter

This chapter introduces you to user accounts and to how to plan them. It also presents the skills and knowledge necessary to create local user accounts and to set properties for them.

Before You Begin

To complete this chapter, you must have

- A computer that meets the minimum hardware requirements listed in "[Hardware Requirements](#)."
- Windows 2000 Professional installed on the computer.

[\[Previous\]](#) [\[Next\]](#)

Lesson 1: Understanding User Accounts

Microsoft Windows 2000 provides three different types of user accounts: local user accounts, domain user accounts, and built-in user accounts. A *local user account* allows a user to log on to a specific computer to gain access to resources on that computer. A *domain user account* allows a user to log on to the domain to gain access to network resources. A *built-in user account* allows a user to perform administrative tasks or to gain access to local or network resources.

After this lesson, you will be able to

- Describe the role and purpose of user accounts.

Estimated lesson time: 10 minutes

Local User Accounts

Local user accounts allow users to log on at and gain access to resources only on the computer where you create the local user account. When you create a local user account, Windows 2000 creates the account *only* in that computer's security database, which is called the *local security database*, as shown in Figure 10.1. Windows 2000 doesn't replicate local user account information to any other computer. After the local user account exists, the computer uses its local security database to authenticate the local user account, which allows the user to log on to that computer.



Local user accounts

- Provide access to resources on the local computer
- Are created only on computers that are not in a domain
- Are created in the local security database

Figure 10.1 *Characteristics of local user accounts*

If you have a workgroup that consists of five computers running Windows 2000 Professional and you create a local user account—for example, User1 on Computer1—you can log on to Computer1 only with the User1 account. If you need to be able to log on to all five of the computers in the workgroup as User1, you must create a local user account, User1, on each of the five computers. Furthermore, if you decide to change the password for User1, you must change the password for User1 on each of the five computers because each of these computers maintains its own local security database.

NOTE

Do not create local user accounts on computers running Windows 2000 that are part of a domain because the domain doesn't recognize local user accounts. Therefore, the user is unable to gain access to resources in the domain and the domain administrator is unable to administer the local user account properties or assign access permissions for domain resources.

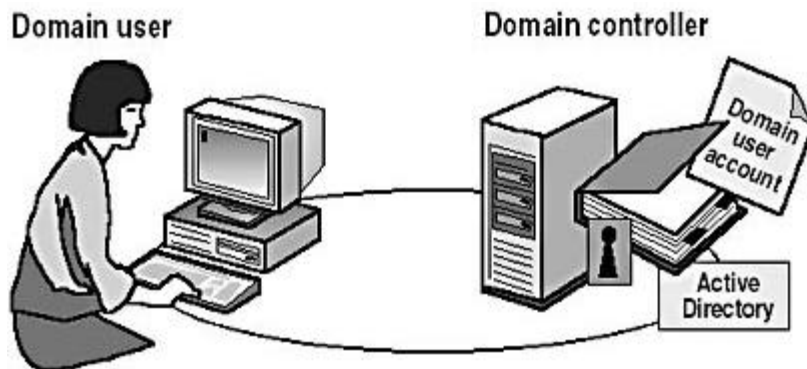
Domain User Accounts

Domain user accounts allow users to log on to the domain and gain access to resources anywhere on the network. The user provides his or her password and user name during the logon process. By using this information, Windows 2000 authenticates the user and then builds an access token that contains information about the user and security settings. The access token identifies the user to computers running Windows 2000 on which the user tries to gain access to resources. Windows 2000 provides the access token for the duration of the logon session.

NOTE

You can have domain user accounts only if you have a domain. You can have a domain only if you have at least one computer running one of the Windows 2000 Server products that is configured as a domain controller, which has the directory services based on Active Directory technology installed.

You create a domain user account in the copy of the Active Directory database (the Directory) on a domain controller, as shown in Figure 10.2. The domain controller replicates the new user account information to all domain controllers in the domain. After Windows 2000 replicates the new user account information, all of the domain controllers in the domain tree can authenticate the user during the logon process.



Domain user accounts

- Provide access to network resources
- Provide the access token for authentication
- Are created in Active Directory directory services on a domain controller

Figure 10.2 *Characteristics of domain user accounts*

Built-In User Accounts

Windows 2000 automatically creates accounts called *built-in accounts*. Two commonly used built-in accounts are Administrator and Guest.

Administrator

Use the built-in Administrator account to manage the overall computer. If your computer is part of a domain, use the built-in Administrator account to manage the domain configuration. Tasks done using the Administrator account include creating and modifying user accounts and groups, managing security policies, creating printers, and assigning permissions and rights to user accounts to gain access to resources.

If you are the administrator, you should create a user account that you use to perform nonadministrative tasks. Log on by using the Administrator account only when you perform administrative tasks.

NOTE

You can't delete the Administrator account. As a best practice, you should always rename the built-in Administrator account to provide a greater degree of security. Use a name that doesn't identify it as the Administrator account. This makes it difficult for unauthorized users to break into the Administrator account because they don't know which user account it is.

Guest

Use the built-in Guest account to give occasional users the ability to log on and gain access to resources. For example, an employee who needs access to resources for a short time can use the Guest account.

NOTE

The Guest account is disabled by default. Enable the Guest account only in low-security networks and always assign it a password. You can rename the Guest account, but you can't delete it.

Lesson Summary

In this lesson, you learned that Microsoft Windows 2000 provides local user accounts and built-in user accounts. With a local user account, a user logs on to a specific computer to gain access to resources on that computer. With built-in user accounts, you can perform administrative tasks or gain access to resources.

When you create a local user account, Windows 2000 creates the account only in that computer's security database, which is called the local security database. If you need to have access to multiple computers in your workgroup, you must create an account on each of the computers in the workgroup. You don't create built-in user accounts; Windows 2000 automatically creates them.

You also learned that if your computer is part of a domain, Windows 2000 provides domain user accounts. With a domain user account, a user can log on to the domain to gain access to network resources. And built-in user accounts exist that are domain user accounts and are used to perform administrative tasks or gain access to network resources. When you create a domain user account, Windows 2000 creates the account in the copy of the Active Directory database (the Directory) on a domain controller. The domain controller then replicates the new user account information to all domain controllers in the domain, simplifying user account administration.

[\[Previous\]](#) [\[Next\]](#)

Lesson 2: Planning New User Accounts

You can streamline the process of creating user accounts by planning and organizing the information for the user accounts. You should plan the following areas:

- Naming conventions for user accounts
- Requirements for passwords

After this lesson, you will be able to

- Plan a strategy for creating new user accounts.

Estimated lesson time: 5 minutes

Naming Conventions

The naming convention establishes how users are identified in the domain. A

consistent naming convention will help you and your users remember user logon names and locate them in lists. Table 10.1 summarizes some points you might want to consider in determining a naming convention for your organization.

Table 10.1 *Naming Convention Considerations*

Consideration	Explanation
User logon names must be unique	Local user account names must be unique on the computer where you create the local user account. User logon names for domain user accounts must be unique to the Directory.
Use 20 characters maximum	User logon names can contain up to 20 uppercase or lowercase characters; the field accepts more than 20 characters, but Windows 2000 recognizes only the first 20.
Avoid invalid characters	The following characters are invalid: " / \ [] : ; = , + * ? < >
User logon names are not case sensitive	You can use a combination of special and alphanumeric characters to help uniquely identify user accounts. User logon names are <i>not</i> case sensitive, but Windows 2000 preserves the case.
Accommodate employees with duplicate names	If two users were named John Doe, you could use the first name and the last initial, and then add additional letters from the last name to differentiate the duplicate names. In this example, one user account logon name could be Johnd and the other Johndo. Another possibility would be to number each user logon name—for example, Johnd1 and Johnd2.
Identify the type of employee	In some organizations, it is useful to identify temporary employees by their user account. To identify temporary employees, you can use a T and a dash in front of the user's logon name—for example, T-Johnd. Alternatively, use parentheses in the name—for example, John Doe (Temp).

Password Requirements

To protect access to the computer, every user account should have a password. Consider the following guidelines for passwords:

- Always assign a password for the Administrator account to prevent unauthorized access to the account.
- Determine whether the Administrator or the users will control passwords. You can assign unique passwords for the user accounts and prevent users from changing them, or you can allow users to enter their own passwords the first time they log on. In most cases, users should control their passwords.
- Use passwords that are hard to guess. For example, avoid using passwords with an obvious association, such as a family member's name.
- Passwords can be up to 128 characters; a minimum length of eight characters is

recommended.

- Use both uppercase and lowercase letters, numerals, and valid nonalphanumeric characters. Table 10.1 lists the invalid nonalphanumeric characters.

Lesson Summary

In this lesson, you learned that in planning user accounts, you should determine naming conventions for user accounts, requirements for passwords, and account options such as logon hours, the computers from which users can log on, and account expiration. You learned that domain user accounts can be up to 20 characters long and must be unique within the OU where you create the domain user account. Local user account names can also be up to 20 characters long and must be unique on the computer where you create the local user account. Making these decisions before you start creating user accounts will reduce the amount of time it takes to create the needed user accounts and will simplify managing these accounts.

[\[Previous\]](#) [\[Next\]](#)

Lesson 3: Creating User Accounts

Use the Computer Management snap-in to create a new local user account. When you create a local user account, it is always created in the local security database of that computer.

After this lesson, you will be able to

- Create a local user account.

Estimated lesson time: 10 minutes

The Computer Management Snap-In

The Computer Management snap-in (illustrated in Figure 10.3) is the tool you use to create local user accounts.

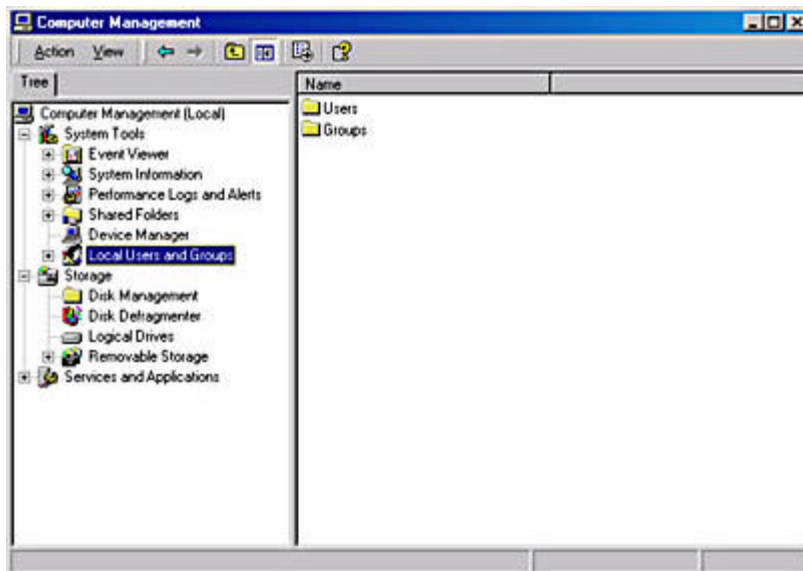


Figure 10.3 *The Computer Management snap-in*

You can create local user accounts by doing the following:

1. Click the Start button, point to Programs, point to Administrative Tools, and then click Computer Management.
2. In the Computer Management window, in the console pane, click Local Users And Groups.
3. In the details pane, right-click Users, and then click New User.
4. Fill in the appropriate fields in the New User dialog box (see Figure 10.4), and then click Create.

Table 10.2 describes the local user account options shown in Figure 10.4.

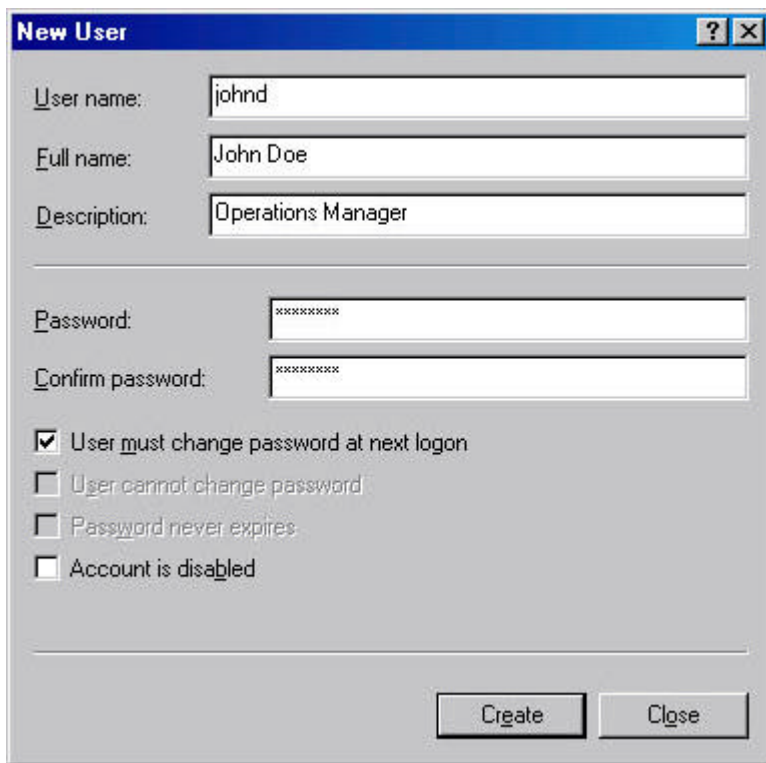


Figure 10.4 *The New User dialog box*

Table 10.2 *Local User Account Options*

Option	Description
User Name	The user's logon name. This field is required.
Full Name	The user's full name. This includes the user's first and last names but can also include the middle name or initial.
Description	An optional field that allows you to type descriptive text about the user account or the user.
Password	The password that is used to authenticate the user. For greater security, <i>always</i> assign a password. Notice that you don't see the password. It is represented as asterisks when you type the password, regardless of the length of the password.
Confirm Password	Confirm the password by typing it a second time to make sure that you typed the password correctly. This is required if you assign a password.
User Must Change Password At Next Logon	Select this check box if you want the user to change his or her password the first time that he or she logs on. This ensures that the user is the only person who knows the password. By default, this check box is selected.
User Cannot Change Password	Select this check box if you have more than one person using the same user account (such as Guest) or to maintain control over user account passwords. This allows only administrators to control passwords. When the User Must Change Password At Next Logon check box is selected, the User Cannot Change

Password check box isn't available.

Password Never Expires	Select this check box if you never want the password to change—for example, for a user account that will be used by a program or a Windows 2000 service. The User Must Change Password At Next Logon check box overrides the Password Never Expires check box. When the User Must Change Password At Next Logon check box is selected, the Password Never Expires check box isn't available.
Account Is Disabled	Select this check box to prevent use of this user account—for example, for a new employee who hasn't started yet.

NOTE

Always require new users to change their passwords the first time they log on. This will force them to use passwords that only they know.

TIP

For added security on networks, create random initial passwords for all new user accounts by using a combination of letters and numbers. Creating a random initial password will help keep the user account secure.



Practice: Creating Local User Accounts

In this practice, you will create the user accounts shown in the following table. Then you will test the logon procedure with one of the users you created.

User name	Full name	Password	Change password
User1	User One	(blank)	Must
User2	User Two	(blank)	(blank)
User3	User Three	User3	Must
User4	User Four	User4	(blank)

The following procedure outlines the steps that are required to create the first user account by using the Computer Management snap-in. After you have created the first user account, follow the same steps to create the remaining user accounts and use the information in the table to set them up.

- **To create a local user account**

1. Log on as Administrator.
2. Click the Start button, point to Programs, point to Administrative Tools, and then

click Computer Management.

Windows 2000 displays the Computer Management snap-in.

3. Expand Local Users And Groups.
4. Right-click Users, and then click New User.

Windows 2000 displays the New User dialog box.

5. Type **User1** in the User Name box.
6. Type **User One** in the Full Name box.
7. In the Password box and the Confirm Password box, type the password or leave these boxes blank if you aren't assigning a password.

If you enter a password, notice that the password is displayed as asterisks as you type. This prevents onlookers from viewing the password as it is entered.

In high-security environments, assign initial passwords to user accounts and then require users to change their password the next time that they log on. This prevents a user account from existing without a password, and once the user logs on and changes his or her password, only the user knows the password.

8. Specify whether or not the user can change his or her password.
9. After you have selected the appropriate password options, click Create.

The New User dialog box clears and remains displayed so that you can create another user account.

10. Complete steps 5-9 for the remaining user accounts.
11. When you finishing creating users, click Close to close the New User dialog box.
12. Close the Computer Management window.

- **To test a local user account**

1. Log off as Administrator.
2. Log on as User1 with no password.

A Logon Message box appears informing you that you are required to change your password at first logon.

3. Click OK
4. When prompted to change User1's password, leave the Old Password box empty, type **password** in the Password and Confirm New Password boxes, and then click OK.

A Change Password dialog box appears.

5. Click OK.

Lesson Summary

In this lesson, you learned how to use the Computer Management snap-in to create a new local user account. When you create a local user account, it is only created in the local security database of that computer. You can configure options for the accounts you create, including a user name, a full name, and a description. You can also configure password options such as whether users must change their passwords at the next logon, whether users can ever change their passwords, and whether the passwords expire. In the practice portion of this lesson, you created four local user accounts.

[\[Previous\]](#) [\[Next\]](#)

Lesson 4: Setting Properties for User Accounts

A set of default properties is associated with each local user account that you create. After you create a local user account, you can configure these account properties. A user's Properties dialog box has three tabs that contain information about each user account: the General tab, the Member Of tab, and the Profile tab.

After this lesson, you will be able to

- Set properties for user accounts.

Estimated lesson time: 15 minutes

The General Tab in a User Account's Properties

The General tab in the Properties dialog box for a user account (see Figure 10.5) allows you to set or edit all the fields from the New User dialog box, except for User Name, Password, and Confirm Password. It also provides one additional check box: Account Is Locked Out.

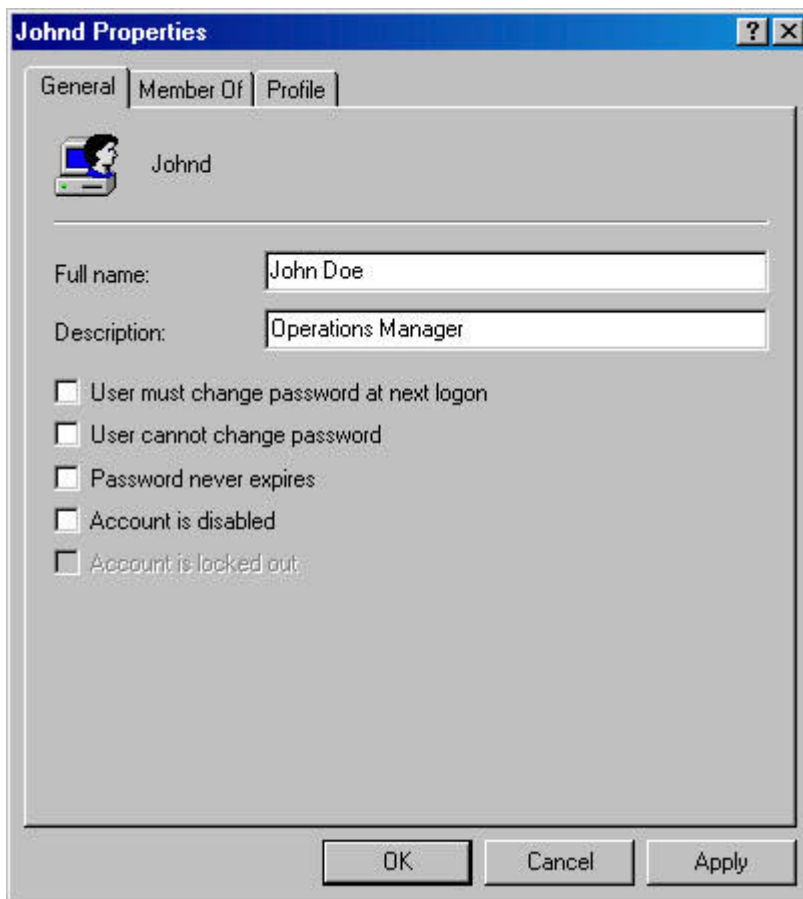


Figure 10.5 *The General tab of a user's Properties dialog box*

You can't select the Account Is Locked Out check box because it is unavailable when the account is active and not locked out of the system. The system locks out a user if he or she exceeds the limit set on the number of failed logon attempts. This is a security feature to make it more difficult for an unauthorized user to break into the system. If an account has been locked out by the system, the Account Is Locked Out check box becomes available and an administrator can clear the check box to allow the user access to the system.

The Member Of Tab in a User Account's Properties

The Member Of tab in the Properties dialog box for a user account allows you to add the user account to or remove the user account from a group. For information on groups, see [Chapter 11](#), "Setting Up and Managing Groups."

The Profile Tab in a User Account's Properties

The Profile tab in the Properties dialog box for a user account allows you to set a path for the user profile, logon script, and home folder (see Figure 10.6).

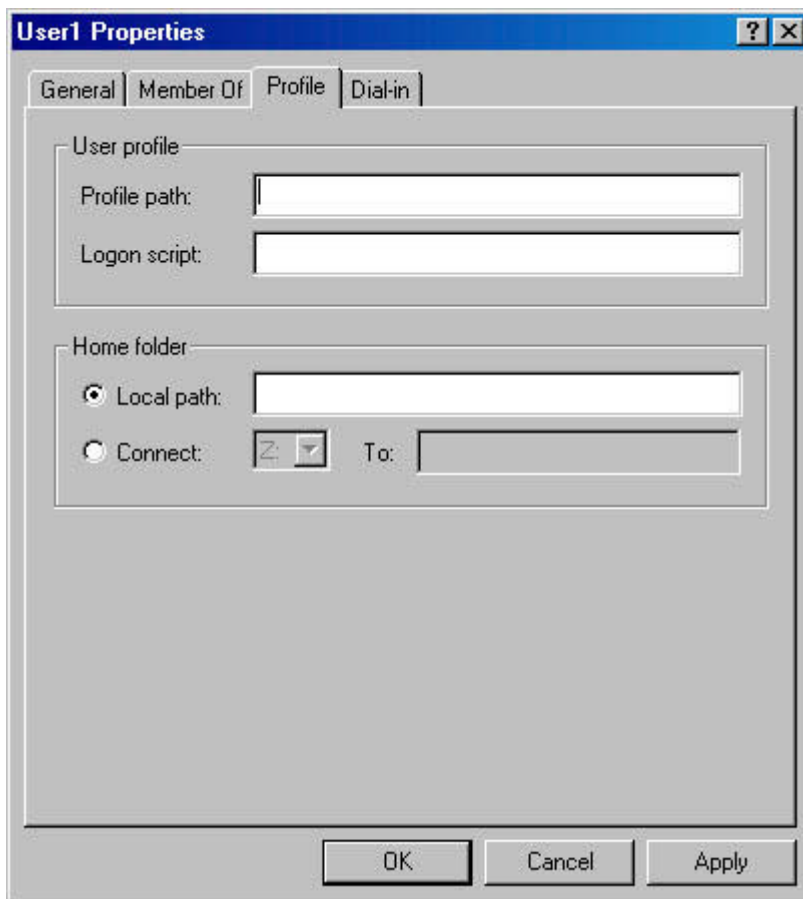


Figure 10.6 *The Profile tab of a user's Properties dialog box*

User Profile

A *user profile* is a collection of folders and data that stores the user's current desktop environment and application settings, as well as personal data. A user profile also contains all of the network connections that are established when a user logs on to a computer, such as Start-menu items and mapped drives to network servers. User profiles maintain consistency for users in their desktop environments by providing each user the same desktop environment that he or she had the last time that he or she logged on to the computer.

Windows 2000 creates a user profile the first time that a user logs on at a computer. After the user logs on for the first time, Windows 2000 stores the user profile on that computer. This user profile is also known as a *local user profile*.

User profiles operate in the following manner:

- When a user logs on to a client computer running Windows 2000, the user always receives his or her individual desktop settings and connections, regardless of how many users share the same client computer.
- The first time that a user logs on to a client computer running Windows 2000, Windows 2000 creates a default user profile for the user and stores it in the system partition root\Documents and Settings*user_logon_name* folder (typically C:\Documents and Settings*user_logon_name*), where *user_logon_name* is the name the user enters when logging on to the system.

- A user profile contains the My Documents folder, which provides a place for users to store personal files. My Documents is the default location for the File Open and Save As commands. By default, Windows 2000 creates a My Documents icon on the user's desktop. This makes it easier for users to locate their personal documents.
- A user can change his or her user profile by changing desktop settings. For example, a user makes a new network connection or adds a file to My Documents. Then, when the user logs off, Windows 2000 incorporates the changes into the user profile. The next time the user logs on, the new network connection and the file are present.

NOTE

You should have users store their documents in My Documents rather than in home directories. Home directories are covered later in this chapter. Windows 2000 automatically sets up My Documents, and it is the default location for storing data for Microsoft applications.

By opening the System program in Control Panel and clicking the User Profiles tab, an administrator can easily copy, delete, or change the type of a user profile. Changing the type for user profiles allows an administrator to change it from a local user profile, which sets up the user's desktop environment on a specific computer, to a roaming user profile. A *roaming user profile* is especially helpful in a domain environment, because it follows the user around, setting up the same desktop environment for the user no matter what computer the user logs on to in the domain.

There is a third type of user profile, the mandatory user profile, which is a read-only roaming user profile. When the user logs off, Windows 2000 does not save any changes made during the session, so the next time the user logs on the profile is exactly the same as the last time the user logged on. You can create a mandatory user profile for a specific user or to be used with a group of users.

NOTE

A hidden file called Ntuser.dat contains the section of the Windows 2000 system settings that applies to the individual user account and contains the user environment settings. Create a user account that you can use to create user profiles. Log on as the user you created, and configure all the desktop environment settings you want. Log on as administrator and locate the Ntuser.dat file in C:\Documents and Settings\user_logon_name. You make the profile a mandatory roaming user profile by changing its name to Ntuser.man. You can then copy this file to apply the mandatory user profile to any other user or group.

Logon Script

A logon script is a file you can create and assign to a user account to configure the user's working environment. For example, a login script can be used to establish network connections or start applications. Each time a user logs on, the assigned logon script is run.

Home Folder

In addition to the My Documents folder, Windows 2000 provides you with the means to create another location for users to store their personal documents. This additional location is the user's home folder. You can store a home folder on a client computer or in a shared folder on a file server. In fact, you can locate all users' home folders in a central location on a network server.

Storing all home folders on a file server provides the following advantages:

- Users can gain access to their home folders from any client computer on the network.
- The backing up and administration of user documents is centralized.
- The home folders are accessible from a client computer running any Microsoft operating system (including MS-DOS, Windows 95, Windows 98, and Windows 2000).

NOTE

Store home folders on an NTFS file system volume so that you can use NTFS permissions to secure user documents. If you store home folders on a FAT volume, you can restrict home folder access only by using shared folder permissions.

To create a home folder on a network file server, you must perform the following three tasks:

1. Create and share a folder in which to store all home folders on a network server. The home folder for each user will reside in this shared folder.
2. For the shared folder, remove the default Full Control permission from the Everyone group and assign Full Control to the Users group. This ensures that only users with domain user accounts can gain access to the shared folder.
3. Provide the path to the user's home folder in the shared home directory folder on the Profile tab of the Properties dialog box for the user account. Since the home folder is on a network server, click Connect and specify a drive letter to use to connect. In the To box, you would specify a UNC name—for example, `\\server_name\shared_folder_name\user_logon_name`. Type the *username* variable as the user's logon name to automatically name each user's home folder the user logon name (for example, type `\\server_name\Users\%username%`).

If you use the *username* variable to name a folder on an NTFS volume, the user is assigned the NTFS Full Control permission, and all other permissions are removed for the folder, including those for the Administrator account.

You can set User Account Properties by doing the following:

1. On the Administrative Tools menu, click Computer Management.
2. Right-click the appropriate local user account, and then click Properties.
3. Click the appropriate tab for the properties that you want to enter or change, and then enter values for each property.



Practice: Modifying User Account Properties

In this practice, you will modify user account properties. Then you will test them.

Exercise 1: Testing Account Properties

In this exercise, you will again test the User Must Change Password At Next Logon property that you configured when you created users in the previous Practice. You will then set the User Cannot Change Password Account property on User1 and the Account Is Disabled property on User2, and then test these account properties.

- **To test User Must Change Password At Next Logon Property**

1. If a user is currently logged on to your computer, log that user off.
2. Log on to the system as User3. Remember to use this user's password: User3.

Windows 2000 displays a Logon Message dialog box indicating that you are required to change your password at first logon.

3. Click OK.

Windows 2000 displays a Change Password dialog box. Notice that the password you just typed is in the Old Password box.

4. Type **password** in both the New Password box and in the Confirm New Password box.
5. Click OK.

Windows 2000 displays a Change Password dialog box indicating that your password has been changed.

6. Click OK.

Exercise 2: Setting User Account Properties

In this exercise, you will set and then test the User Cannot Change Password property.

- **To set the User Cannot Change Password Property**

1. Log off as User3.
2. Log on as Administrator.
3. Start Computer Management from the Administrative Tools menu.

4. Expand Local Users And Groups, and then click Users.

Windows 2000 displays the users in the details pane.

5. Right-click User1 and then click Properties.

The User1 Properties dialog box appears.

6. Select User Cannot Change Password.

The User Cannot Change Password check box should contain a check mark, indicating that it is selected. Notice that the User Must Change Password At Next Logon check box is now unavailable.

7. Click OK to close the User1 Properties dialog box.

8. Right-click User2, and then select Properties.

The User2 Properties dialog box appears.

9. Select Account Is Disabled.

The Account Is Disabled check box should contain a check mark, indicating that it is selected.

10. Click OK to close the User2 Properties dialog box, close Computer Management, and then log off the computer.

- **To test User Account Properties**

1. Log on as User1 with a password of password.

2. Press Ctrl+Alt+Delete.

Windows 2000 displays the Windows Security dialog box.

3. Click Change Password.

The Change Password dialog box appears.

4. Type **password** in the Old Password box, and then type **User1** in the New Password and the Confirm New Password boxes.

5. Click OK.

A Change Password dialog box appears indicating that you do not have permission to change your password.

6. Click OK.

7. Click Cancel to close the Change Password dialog box.

8. Log off as User1 and then log on as User2 with no password.

A Logon Message dialog box appears, indicating that your account has been disabled.

9. Click OK to close the Logon Message dialog box.

Lesson Summary

In this lesson, you learned that a set of default properties is associated with each local user account that you create. These properties include whether users can change their own password, whether users are required to change their password at the next logon, and whether the account is disabled. The Computer Management snap-in allows you to easily configure or modify these account properties.

In the practice portion of this lesson, you were able to configure account properties, including prohibiting users from changing their passwords and disabling a user account. Finally, you tested these properties to verify that they worked as expected.

[\[Previous\]](#) [\[Next\]](#)

Review



The following questions will help you determine whether you have learned enough to move on to the [next chapter](#). If you have difficulty answering these questions, please go back and review the material in this chapter before beginning the next chapter. See [Appendix A](#), "Questions and Answers," for the answers to these questions.

1. Where does Windows 2000 create local user accounts?
2. What different capabilities do domain user accounts and local user accounts provide to users?
3. What should you consider when you plan new user accounts?
4. What information is required to create a local user account?
5. What are built-in accounts and what are they used for?

[Answers](#)