Server
Enterprise

CHAPTER

8

Managing Account Policy, User Rights, and Auditing

About Chapter 8

This chapter explores the Policies menu in Windows NT User Manager/User Manager for Domains, with emphasis on its three major configurable options: Account Policy, User Rights, and Auditing.

Managing account policy, which applies to all users in the domain, is discussed first. Password restrictions and the account lockout feature are also addressed.

Next, the chapter explains how to manage user rights, which enable users to perform tasks. All the Windows NT user rights are listed and described in this section, followed by detailed, step-by-step instructions for assigning user rights.

Finally, Chapter 8 explores auditing, the Windows NT feature that, when enabled, produces a log of specified events and activities.

This chapter includes two hands-on labs. In the first lab, you implement Windows NT auditing, and then view audit events in the security log in Event Viewer. In the second, you set account policies and configure user rights.

Chapter 8 is optional if you're preparing only for the Workstation exam, but essential if you're preparing for either the Server or Enterprise exams. This chapter maps to the "Manage user and group accounts" objective in the Managing Resources section in the Server and Enterprise exams' objectives.

Managing Account Policy

This chapter focuses on the Policies menu in User Manager (on Windows NT Workstation computers) and User Manager for Domains (on Windows NT Server computers). The Policies menu provides three main configurable options: Account Policy, User Rights, and Auditing. Only members of the Administrators local group have the necessary rights to manage account policy, user rights, and auditing.

The Account Policy dialog box has two main sections: one enables you to configure password restrictions, and another enables you to set the account lockout policy.

Settings in the Account Policy dialog box apply to *all* users in the domain (or to all users on a computer, if it is not a domain controller). You can't set individual account policies.

TO ACCESS THE ACCOUNT POLICY 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, select Policies ➪ Account. The Account Policy dialog box appears, as shown in Figure 8-1. Notice the default settings in this dialog box.

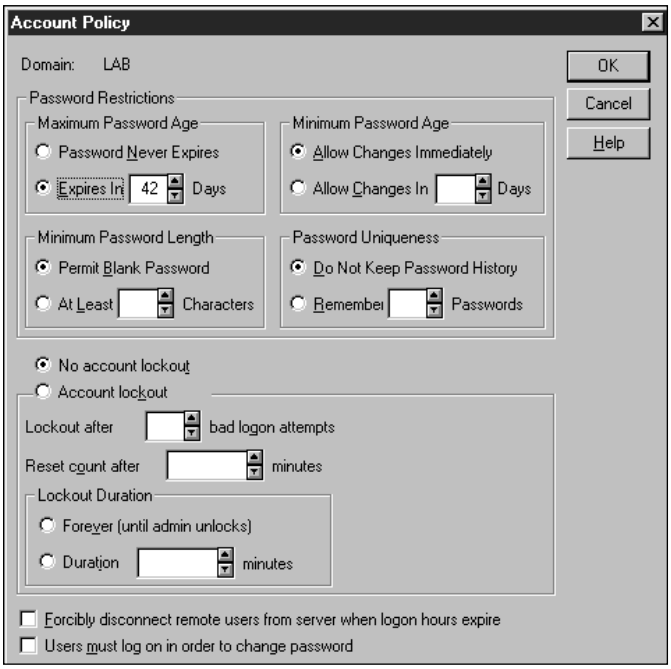


FIGURE 8-1 **The Account Policy dialog box in User Manager for Domains**

Password restrictions

The Password Restrictions section of the Account Policy dialog box has four configurable options: Maximum Password Age, Minimum Password Age, Minimum Password Length, and Password Uniqueness.

Maximum Password Age

Maximum Password Age determines the maximum number of days a user may use the same password. Two selections are available in this section: Password Never Expires, or Expires In *xx* Days. The default setting is Expires in 42 Days.

When Password Never Expires is selected, users are never required to change their passwords.

When Expires in *xx* Days is selected, Windows NT forces users to change their passwords when the maximum password age setting is exceeded. Normal

settings for password expiration are between thirty and ninety days. If users have to change their passwords too frequently, they may be unable to remember their passwords.

If a user's password expires *and* the check box next to "Users must log on in order to change password" (at the bottom of the dialog box) is selected, the user will *not* be able to change his or her own password — the administrator must change the user's password.

in the real world 

I normally recommend administrators do *not* select the check box next to "Users must log on in order to change password," because Windows NT does not give users any warning that their passwords are about to expire. When users attempt to log on after password expiration, they are unable to log on to change their passwords. This situation creates a lot of hassle and extra work for the administrator.

Minimum Password Age

Minimum Password Age determines the minimum number of days a user must keep the same password. Two selections are available in this section: Allow Changes Immediately, or Allow Changes in *xx* Days. The default setting is Allow Changes Immediately.

If Allow Changes Immediately is selected, users can change their passwords as often as they like, without waiting for any time to pass before selecting a new password.

If Allow Changes in *xx* Days is selected, users must use their passwords for at least the number of days specified before Windows NT lets them change their passwords. Normal settings for Minimum Password Age are from one day to the number of days specified as the Maximum Password Age.

If Minimum Password Age is not set, and Password Uniqueness is set at Remember 8 Passwords, then users are often tempted to bypass the Password Uniqueness setting by changing their passwords nine times, in rapid succession, so they can recycle back to their original, favorite, and easily remembered password.

Minimum Password Length

Minimum Password Length specifies the minimum number of characters required in users' passwords. Two selections are possible in this section: Permit Blank Password, or At Least *xx* Characters.

If Permit Blank Password is selected, users are not required to have a password. This is the default setting.

If At Least *xx* Characters is selected, you can specify the minimum number of characters a user's password must contain. Windows NT will not enable users to choose a password with fewer than the required number of characters. Possible settings for password length are from one to fourteen characters. I recommend you set a minimum of eight characters for Minimum Password Length. With a password length of eight characters or more, (assuming basic password security measures are taken) it's statistically almost impossible for an unauthorized user to guess a password.

Password Uniqueness

Password Uniqueness specifies how many different passwords a user must use before an old password can be reused. Two selections are possible in this section: Do Not Keep Password History, or Remember *xx* Passwords. The default setting is Do Not Keep Password History.

If Do Not Keep Password History is selected, users can cycle back and forth between their two favorite passwords each time they are required to change their passwords.

If Remember *xx* Passwords is selected, users must use at least the number of new passwords specified before they can reuse an old password. Possible settings for Password Uniqueness are between one and twenty-four passwords. Normal settings range between five and twelve passwords.

You can multiply the number of passwords specified in Password Uniqueness times the number of days specified in Minimum Password Age to determine the number of days that must pass before a user can reuse an old password.

For more password tips, see the "Passwords" section in Chapter 7.

Account lockout

The Account lockout section of the Account Policy dialog box specifies how Windows NT treats user accounts after several successive unsuccessful logon attempts have occurred. The default setting is "No account lockout."

Figure 8-2 shows the Account Policy dialog box. Notice the options in the Account lockout section.

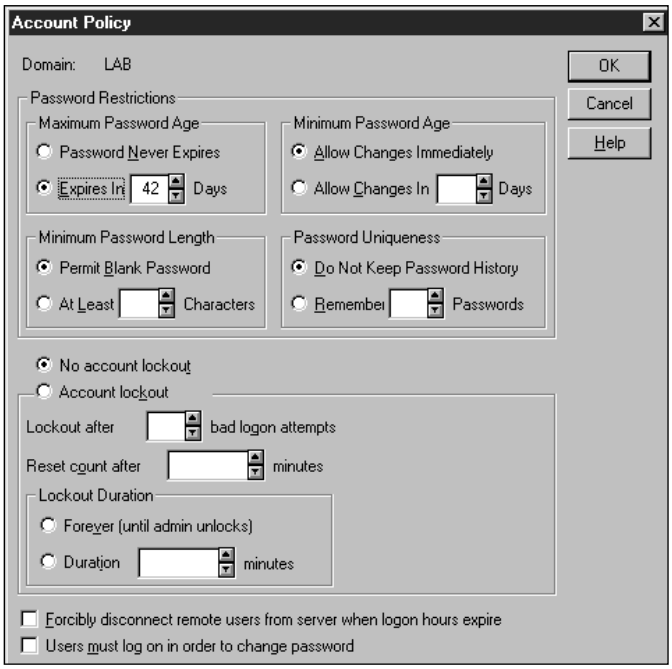


FIGURE 8-2 The Account Policy dialog box in User Manager for Domains

When "No account lockout" is selected, user accounts are never locked out. This means no matter how many unsuccessful logon attempts a user makes, the user's account is not locked out.

When Account lockout is selected, users are locked out after the specified number of successive bad logon attempts is reached. Several configuration options exist for Account lockout: Lockout after *xx* bad logon attempts, Reset count after *xx* minutes, and Lockout Duration.

Lockout after *xx* bad logon attempts specifies the number of successive unsuccessful logon attempts that are acceptable before Windows NT will lock out an account. The possible settings are from one to 999 bad logon attempts. Normal settings for this configuration are from three to ten bad logon attempts. This counter is reset after each successful logon. Windows NT maintains a separate counter for each user account.

Reset count after *xx* minutes specifies the number of minutes that must pass without a bad logon attempt in order for the bad logon attempts counter to be reset to zero. (Resetting the counter to zero gives users the full number of possible bad

logon attempts before account lockout.) The possible settings are from one to 99,999 minutes. Normal settings for this configuration are from thirty to sixty minutes.

Lockout duration specifies how long a user account is locked out after the specified number of bad logon attempts occurs. Two possible settings are in this section: Forever (until admin unlocks), or "Duration *xx* minutes."

If Forever is selected *and* the specified number of bad logon attempts occurs, the administrator must unlock the user account in User Manager (or User Manager for Domains) before the user can log on.

If "Duration *xx* minutes" is selected, user accounts that are locked out (because the specified number of bad logon attempts have been exceeded) are unlocked automatically by Windows NT after the specified number of minutes elapses. The possible settings are from one to 99,999 minutes. Normal settings for this configuration are from thirty to sixty minutes.

Two additional check boxes are in the Account Policy dialog box: "Forcibly disconnect remote users from server when logon hours expire," and "Users must log on to change password." By default, both of these check boxes are *not* selected. The "Forcibly disconnect remote users from server when logon hours expire" check box is only available on Windows NT Server computers configured as domain controllers.

If "Forcibly disconnect remote users from server when logon hours expire" is selected, users whose logon hours expire are automatically disconnected from the domain controllers in the domain. Users are not disconnected from Windows NT Workstation computers, however, or from member servers in the domain.

If "Users must log on in order to change password" is selected, and a user's password expires, the administrator must change the user's password (because the user cannot log on with an expired password).

A configuration conflict arises when the "Users must log on in order to change password" option is set in Account Policy *and* new users are configured so that User Must Change Password at Next Logon. This combination of settings places users in a catch-22 situation: Users can't log on without changing their passwords, and users can't change their passwords without logging on. The administrator can resolve this problem by changing the users' passwords and clearing the check box next to User Must Change Password at Next Logon in the users' Properties dialog box in User Manager (or User Manager for Domains).

Managing User Rights

User rights authorize users and groups to perform specific tasks on a Windows NT computer. User rights are not the same as permissions: user rights enable users to *perform tasks*; whereas permissions enable users to *access objects*, such as files, folders, and printers.

User rights are assigned in the User Rights Policy dialog box in User Manager or User Manager for Domains.

TO ACCESS THE USER RIGHTS POLICY 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, select Policies ➪ User Rights.

Figure 8-3 shows the User Rights Policy dialog box. Notice the option to Show Advanced User Rights.

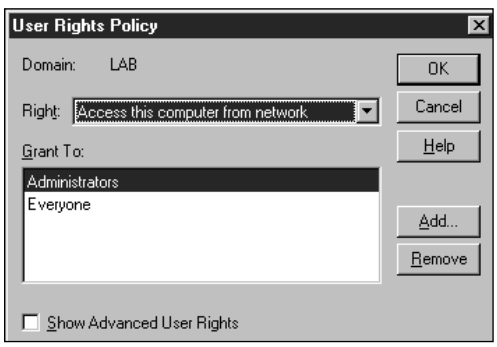


FIGURE 8-3 **The User Rights Policy dialog box in User Manager for Domains**

The following sections discuss user rights and advanced user rights and examine how user rights are assigned.

User Rights

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

User rights are listed in the User Rights Policy Dialog box. You can choose to display regular user rights or a combination of regular and advanced user rights in the Right drop-down list box. The default configuration displays only non-advanced user rights.

Table 8-1 lists and describes each of the Windows NT user rights. The table also indicates whether each right is an advanced user right.

TABLE 8-1 WINDOWS NT USER RIGHTS

USER RIGHT	*ADVANCED USER RIGHT?*	*DESCRIPTION*
Access this computer from the network	No	Authorizes a user to access a computer over the network.
Act as part of the operating system	Yes	Not normally used by administrators. Used by programmers of Windows NT applications. See Microsoft's Win32 Software Development Kit for more information.
Add workstations to domain	No	Authorizes a user to cause workstation computers to join the domain.
Back up files and directories	No	Authorizes a user to back up files and folders. This right supersedes permissions on files and folders.
Bypass traverse checking	Yes	Authorizes a user to change the current folder on the user's computer to a different folder, even if the user or group has no permissions to the newly selected current folder.
Change the system time	No	Authorizes a user to change the time on the Windows NT computer's internal clock.
Create a pagefile	Yes	Not normally used by administrators. Used by programmers of Windows NT applications. See Microsoft's Win32 Software Development Kit for more information.

USER RIGHT	ADVANCED USER RIGHT?	DESCRIPTION
Create a token object	Yes	Not normally used by administrators. Used by programmers of Windows NT applications. See Microsoft's Win32 Software Development Kit for more information.
Create permanent shared objects	Yes	Not normally used by administrators. Used by programmers of Windows NT applications. See Microsoft's Win32 Software Development Kit for more information.
Debug programs	Yes	Not normally used by administrators. Used by programmers of Windows NT applications. See Microsoft's Win32 Software Development Kit for more information.
Force shutdown from a remote system	No	This right is not currently implemented. It is reserved for future use.
Generate security audits	Yes	Not normally used by administrators. Used by programmers of Windows NT applications. See Microsoft's Win32 Software Development Kit for more information.
Increase quotas	Yes	Not normally used by administrators. Used by programmers of Windows NT applications. See Microsoft's Win32 Software Development Kit for more information.
Increase scheduling priority	Yes	Not normally used by administrators. Used by programmers of Windows NT applications. See Microsoft's Win32 Software Development Kit for more information.
Load and unload device drivers	No	Authorizes a user to load and unload device drivers for the Windows NT operating system.
Lock pages in memory	Yes	Not normally used by administrators. Used by programmers of Windows NT applications. See Microsoft's Win32 Software Development Kit for more information.

continued

TABLE 8-1 *(continued)*

USER RIGHT	ADVANCED USER RIGHT?	DESCRIPTION
Log on as a batch job	Yes	Not normally used by administrators. Used by programmers of Windows NT applications. See Microsoft's Win32 Software Development Kit for more information.
Log on as a service	Yes	Allows a service or application to log on using a specified user account. (For example, in Chapter 4 you configured the Directory Replicator service to use a specific user account to log on as a service.)
Log on locally	No	Authorizes a user to log on locally (interactively at the computer).
Manage auditing and security log	No	Authorizes a user to view and change the security log in Event Viewer. Enables a user to configure auditing of files, folders, and printers. Does *not* enable a user to access the Audit Policy dialog box in User Manager.
Modify firmware environment values	Yes	Not normally used by administrators. Used by programmers of Windows NT applications. See Microsoft's Win32 Software Development Kit for more information.
Profile single process	Yes	Not normally used by administrators. Used by programmers of Windows NT applications. See Microsoft's Win32 Software Development Kit for more information.
Profile system performance	Yes	Not normally used by administrators. Used by programmers of Windows NT applications. See Microsoft's Win32 Software Development Kit for more information.
Replace a process level token	Yes	Not normally used by administrators. Used by programmers of Windows NT applications. See Microsoft's Win32 Software Development Kit for more information.

USER RIGHT	ADVANCED USER RIGHT?	DESCRIPTION
Restore files and directories	No	Authorizes a user to restore files and folders. This right supersedes permissions on files and folders.
Shut down the system	No	Authorizes a user to shut down the Windows NT computer the user is logged on to.
Take ownership of files or other objects	No	Authorizes a user to take ownership of files, folders, and printers.

Assigning user rights

The assigning of user rights is accomplished in the User Rights Policy dialog box. You can add and remove user rights to and from users and groups in this dialog box.

The following sections describe first how to assign a user right to a user or group, and then how to remove a user right from a user or group.

TO ASSIGN A USER RIGHT TO A USER OR GROUP, FOLLOW THESE STEPS:

1. In the User Rights Policy dialog box in User Manager (or User Manager for Domains), select the user right you want to assign from the Right drop-down list box. (If you want to assign an advanced user right, first select the check box next to Show Advanced User Rights.)

   Figure 8-4 shows the User Rights Policy dialog box. Notice the "Back up files and directories" user right is selected. Click the Add command button.

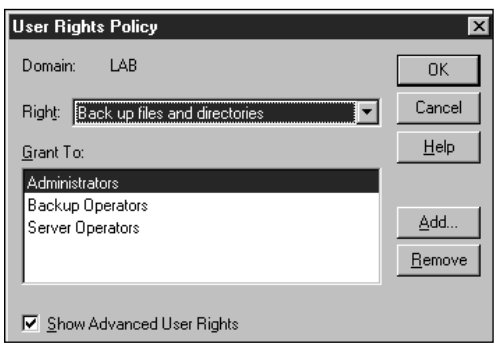


FIGURE 8-4 **Assigning the "Back up files and directories" user right**

2. The Add Users and Groups dialog box appears. If you want to assign a user right to a user, click the Show Users command button. (Otherwise, only groups are listed.) Scroll down through the Names list box and select the user(s) and/or group(s) to which you want to assign a user right.

   Figure 8-5 shows the Add Users and Groups dialog box. Notice both users and groups are displayed in the Names list box (because the Show Users command button has been clicked).

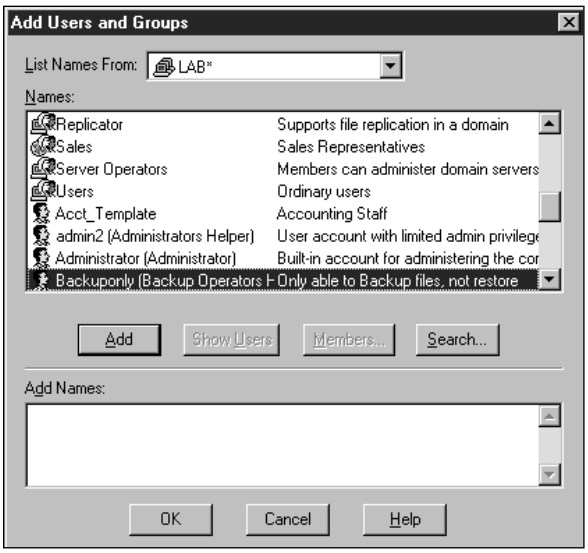


FIGURE 8-5 **The Add Users and Groups dialog box**

   Click the Add command button. (Or, instead of first selecting a user or group and then clicking the Add command button, you can double-click each user or group to which you want to assign the user right.) The name(s) you select appear in the Add Names list box. Click OK.

3. The User Rights Policy dialog box reappears. Click OK.
4. Exit User Manager (or User Manager for Domains).

TO REMOVE A USER RIGHT FROM A USER OR A GROUP, FOLLOW THESE STEPS:

1. In the User Rights Policy dialog box in User Manager (or User Manager for Domains), select the user right you want to remove from the Right drop-down list box. (If you want to remove an advanced user right, first select the check box next to Show Advanced User Rights.)

2. Then highlight the user or group you want to remove the user right from in the Grant To list box. Click the Remove command button. Click OK.
3. Exit User Manager (or User Manager for Domains).

in the real world 

Understanding and being able to use Windows NT user rights is important when preparing for the Microsoft Certified Professional exams. Most user rights, however, are not used by administrators in the real world. In my experience, one of the most common "real world" user right assignments is the "Log on locally" user right to users who need to log on interactively to domain controllers.

Managing Auditing

When enabled, Windows NT auditing produces a log of specified events and activities that occur on a Windows NT computer. Audited events are written to the security log in Event Viewer. Windows NT auditing is divided into two areas: system access and object access. *System access auditing* is configured by using User Manager or User Manager for Domains. *Object access auditing* is configured in the Properties dialog boxes for files, folders, and printers. By default, auditing is turned off.

The next section explains how to enable system access auditing using the Audit Policy dialog box in User Manager or User Manager Domains.

TO ACCESS THE AUDIT POLICY DIALOG BOX AND TO ENABLE AUDITING, 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 Policies ➪ Audit.
3. The Audit Policy dialog box appears. The default setting for this dialog box is Do Not Audit. To enable auditing, select the radio button next to Audit These Events, *and* select at least one Success or Failure check box.

The Audit Policy dialog box is shown in Figure 8-6. Note the radio button next to Audit These Events is selected, and the Success and Failure check boxes for File and Object Access are checked. Click OK.

FIGURE 8-6 **Enabling auditing**

4. Exit User Manager (or User Manager for Domains).

When a Success check box is selected, Windows NT generates an audit event each time a user successfully performs the audited task.

When a Failure check box is selected, Windows NT generates an audit event each time a user attempts to perform an audited task but fails (usually because of a lack of rights or permissions).

When both success and failure auditing are selected, an audit event is generated each time a user attempts to perform an audited task, whether successfully or unsuccessfully.

Table 8-2 lists and describes the types of audit events that can be selected in the Audit Policy dialog box.

TABLE 8-2 WINDOWS NT AUDIT EVENTS

Event	*Description*
Logon and Logoff	A user logs on, logs off, or accesses this Windows NT computer over the network.
File and Object Access	A user accesses a file, folder, or printer configured for auditing. Note: To audit file, folder, or print events, you must enable file and object access auditing *in addition to*

Event	Description
	file, folder, or printer auditing (which is set in Windows NT Explorer or in a printer's Properties dialog box).
Use of User Rights	A user exercises an assigned user right, other than the "Log on locally" or "Access this computer from the network" user rights.
User and Group Management	A user account or group is created, changed, or deleted; or, a user account is renamed, disabled, enabled, or its password is changed.
Security Policy Changes	The user rights, audit, or trust relationship policies are modified or changed.
Restart, Shutdown, and System	A user restarts or shuts down the computer, or a system security or security log event occurs.
Process Tracking	An event, such as program activation, some forms of handle duplication, indirect object accesses, or process exit occurs. This event is not often selected for audit by administrators.

Carefully consider which events you need to audit. If you choose to audit everything, your security log will fill up quickly, primarily with useless information.

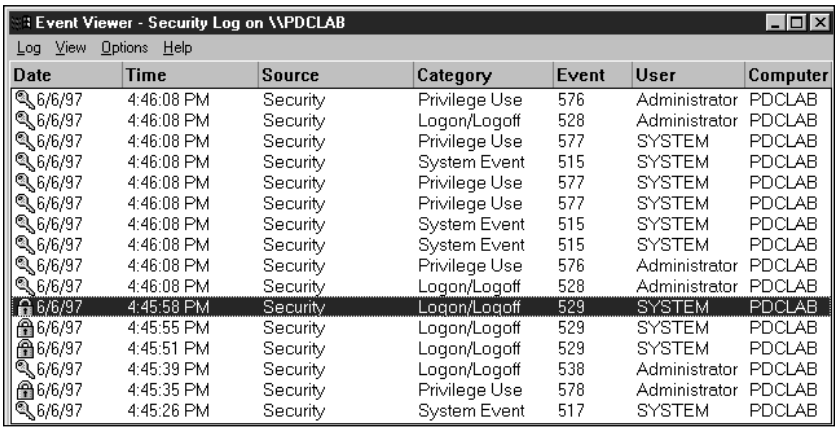
To view audited events in Windows NT, use Event Viewer. The next section describes how to access Event Viewer and view audited events.

TO ACCESS EVENT VIEWER AND TO VIEW SECURITY LOG EVENTS, FOLLOW THESE STEPS:

1. Select Start ≥ Programs ≥ Administrative Tools (Common) ≥ Event Viewer.
2. In the Event Viewer dialog box, select Log ≥ Security.
3. The Security Log dialog box appears.

   Figure 8-7 shows a security log in Event Viewer. Notice some events are marked with keys (these designate success events), and some events are marked with locks (these designate unsuccessful events).

   Double-click an event you want to view in greater detail.
4. The Event Detail dialog box appears. Figure 8-8 shows an Event Detail dialog box. Notice the types of information included in this dialog box.



Date	Time	Source	Category	Event	User	Computer
6/6/97	4:46:08 PM	Security	Privilege Use	576	Administrator	PDCLAB
6/6/97	4:46:08 PM	Security	Logon/Logoff	528	Administrator	PDCLAB
6/6/97	4:46:08 PM	Security	Privilege Use	577	SYSTEM	PDCLAB
6/6/97	4:46:08 PM	Security	System Event	515	SYSTEM	PDCLAB
6/6/97	4:46:08 PM	Security	Privilege Use	577	SYSTEM	PDCLAB
6/6/97	4:46:08 PM	Security	Privilege Use	577	SYSTEM	PDCLAB
6/6/97	4:46:08 PM	Security	System Event	515	SYSTEM	PDCLAB
6/6/97	4:46:08 PM	Security	System Event	515	SYSTEM	PDCLAB
6/6/97	4:46:08 PM	Security	Privilege Use	576	Administrator	PDCLAB
6/6/97	4:46:08 PM	Security	Logon/Logoff	528	Administrator	PDCLAB
6/6/97	4:45:58 PM	Security	Logon/Logoff	529	SYSTEM	PDCLAB
6/6/97	4:45:55 PM	Security	Logon/Logoff	529	SYSTEM	PDCLAB
6/6/97	4:45:51 PM	Security	Logon/Logoff	529	SYSTEM	PDCLAB
6/6/97	4:45:39 PM	Security	Logon/Logoff	538	Administrator	PDCLAB
6/6/97	4:45:35 PM	Security	Privilege Use	578	Administrator	PDCLAB
6/6/97	4:45:26 PM	Security	System Event	517	SYSTEM	PDCLAB

FIGURE 8-7 **Viewing events in the Security Log dialog box**

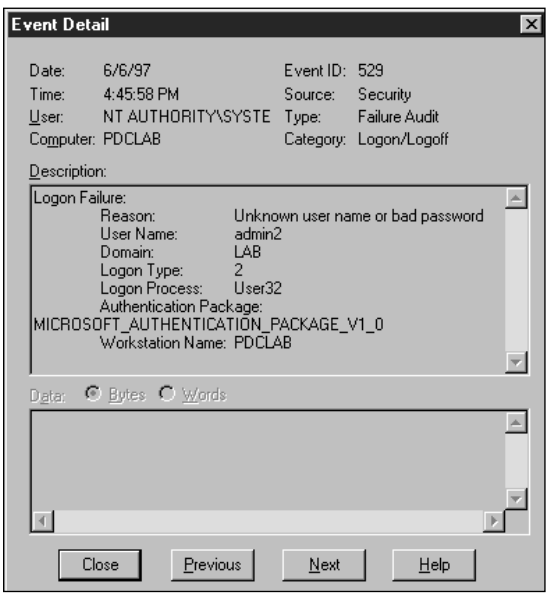


FIGURE 8-8 **Viewing the details of a logon failure event**

Key Point Summary

This chapter focused on the Policies menu in User Manager and User Manager for Domains, which contains three primary configurable options: *Account Policy*, *User Rights*, and *Auditing*.

- Only members of the Administrators local group have the necessary rights to manage account policy, user rights, and auditing.
- The Account Policy dialog box in User Manager or User Manager for Domains has two main sections: One allows you to configure password restrictions, and another allows you to set the account lockout policy. Settings in the Account Policy dialog box apply to *all* users in the domain (or to all users on a computer, if it is not a domain controller.)
  - Four configurable options are in the Password Restrictions section of the Account Policy dialog box: Maximum Password Age, Minimum Password Age, Minimum Password Length, and Password Uniqueness.
  - The Account lockout section of the Account Policy dialog box specifies how Windows NT treats user accounts after several successive bad logon attempts have occurred. Several configurations exist for Account lockout: Lockout after *xx* bad logon attempts, Reset count after *xx* minutes, and Lockout Duration (which can either be set to Forever [until admin unlocks], or Duration *xx* minutes).
  - The two additional check boxes in the Account Policy dialog box include: "Forcibly disconnect remote users from server when logon hours expire," and "Users must log on in order to change password." By default, both of these check boxes are *not* selected.
- *User rights* authorize users or groups to perform specific tasks. User rights, unlike account policy, can be assigned to (and removed from) individual users and groups. User rights are not the same as permissions: User rights enable users to *perform tasks*, whereas permissions enable users to *access objects*, such as files, folders, and printers. User rights are assigned in the User Rights Policy dialog box in User Manager or User Manager for Domains.
  - User rights are made up of advanced and non-advanced rights, such as: Access this computer from the network, Add workstations to domain, Back

up files and directories, Change the system time, Force shutdown from a remote system, Load and unload device drivers, Log on locally, Manage auditing and security log, Restore files and directories, Shut down the system, and Take ownership of files or other objects.

- When enabled, *Windows NT auditing* produces a log of specified events and activities that occur on a Windows NT computer. Audited events are written to the security log in Event Viewer. Auditing is configured in the Audit Policy dialog box in User Manager or User Manager for Domains.
  - When *success auditing* is selected, an audit event is generated every time a user successfully performs the audited task. When *failure auditing* is selected, an audit event is generated each time a user tries to perform an audited task, but fails for some reason. When both success and failure auditing are selected, an audit event is generated every time a user attempts to perform an audited task, whether successfully or unsuccessfully.
  - The events that can be selected for audit in the Audit Policy dialog box are Logon and Logoff; File and Object Access; Use of User Rights; User and Group Management; Security Policy Changes; Restart, Shutdown, and System; and Process Tracking. Audited events can be viewed in the security log in Event Viewer. Remember: To audit file, folder, or print events you must enable file and object access auditing *in addition to* file, folder, or printer auditing (which is set in Windows NT Explorer or in a printer's Properties dialog box).

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 exercises reinforce what you 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 main configurable sections in the Account Policy dialog box?
2. How can you access the Account Policy dialog box?
3. What is the default setting for Maximum Password Age?
4. What does the Minimum Password Age configuration determine?
5. What are the possible settings for Minimum Password Length? What is a recommended setting for Minimum Password Length?
6. What does the Password Uniqueness configuration specify?
7. What does the Account lockout section of the Account Policy dialog box specify?
8. Only members of which local group have the necessary rights to manage account policy, user rights, and auditing?
9. What is the difference between user rights and permissions?
10. When enabled, what does Windows NT auditing produce?
11. Which Windows NT tool can you use to view audited events?
12. In addition to selecting success and/or failure auditing for File and Object Access in the Audit Policy dialog box, what else must you do before you can audit file, folder, or print events?
13. What are the seven specific event types that can be selected for audit in the Audit Policy dialog box?

T/F

14. The settings in the Account Policy dialog box can be configured to apply to individual users. _____
15. User rights can be assigned to individual users and groups. _____

For answers to the Instant Assessment questions see Appendix D.

Hands-on lab exercises

The following hands-on lab exercises provide excellent opportunities to apply the knowledge you've gained in this chapter about Windows NT account policy, user rights, and auditing.

Lab 8.11 *Implementing auditing*

Server Enterprise

The purpose of this lab is to provide you with hands-on experience in using the Windows NT auditing feature.

This lab consists of three parts:

Part 1: Implementing auditing

Part 2: Creating audited events

Part 3: Viewing the security log in Event Viewer

Begin this lab by booting your computer to Windows NT Server. Log on as Administrator.

Perform the following steps carefully.

Part 1: Implementing auditing

In this part you implement auditing on a Windows NT Server computer.

1. Select Start ≥ Programs ≥ Administrative Tools (Common) ≥ User Manager for Domains.
2. In the User Manager dialog box, select Policies ≥ Audit.
3. In the Audit Policy dialog box, select the radio button next to Audit These Events, and then select the Success and Failure check boxes for *all* audit events *except* Process Tracking. Click OK.
4. Auditing is now implemented. Exit User Manager for Domains. Proceed to Part 2.

Part 2: Creating audited events

In this part you cause a user to create audited events.

1. Select Start ≥ Shut Down.
2. In the Shut Down Windows dialog box, select the radio button next to Restart the computer. Click the Yes command button. The computer shuts down and restarts.
3. Reboot the computer to Windows NT Server. Press Ctrl + Alt + Delete to log on. When the Logon Information dialog box appears, type in a user name of **PamR** (replacing Administrator) and a password of **wrongo**. Click OK.
4. An error message appears, stating the system could not log you on. Click OK.
5. The Logon Information dialog box reappears. Type in a password of **newuser**. Click OK.

6. A message appears, indicating you are required to change your password at first logon. (You may recall you set this configuration when you created this user in Lab 7.10.) Click OK.
7. Type in a new password of **password**. Confirm the new password by retyping it. Click OK.
8. A dialog box appears, indicating your password has been changed. Click OK.
9. Another dialog box appears, indicating the local policy of this system does not enable you to log on interactively. Click OK.
10. The Logon Information dialog box reappears. Type in a user name of **Administrator**, and a password of **password**. Click OK. You have now created several audited events. Continue to Part 3.

Part 3: Viewing the security log in Event Viewer

In this part you view the security log in Event Viewer to see the audited events you created in Part 2.

1. Select Start ➢ Programs ➢ Administrative Tools (Common) ➢ Event Viewer.
2. Select Log ➢ Security.
3. Scroll down the list and double-click the first event marked with a lock (not a key) in the left margin. (A lock marks a failure audit event. A key marks a success audit event.)
4. The Event Detail dialog box appears. Notice the event is a logon failure for PamR, because she was not allowed to log on interactively (locally). Click the Close command button.
5. Scroll down and double-click the next event marked with a lock in the left margin.
6. The Event Detail dialog box reappears. This is also a failure audit event. Notice an unexpected error occurred during PamR's attempted logon. Click the Close command button.
7. Scroll down and double-click the next event marked with a lock in the left margin.
8. The Event Detail dialog box appears. This is a logon failure event for PamR, because an incorrect password (wrongo) was entered. Click the Close command button.
9. Double-click various other events, as desired, and view their event details.
10. Exit Event Viewer.

Lab 8.12 *Managing account policy and user rights*

Server Enterprise

The purpose of this lab is to provide you with hands-on experience in setting account policy and user rights in Windows NT.

This lab consists of three parts:

Part 1: Setting account policy

Part 2: Creating users and configuring user rights

Part 3: Auditing revisited — clearing the security log in Event Viewer

Begin this lab by booting your computer to Windows NT Server. Log on as Administrator.

Follow the steps carefully.

Part 1: Setting account policy

In this section you set account policy that affects all users in the domain.

1. Select Start ≥ Programs ≥ Administrative Tools (Common) ≥ User Manager for Domains.
2. In the User Manager dialog box, select Policies ≥ Account.
3. The Account Policy dialog box appears. Configure the following:
   - Configure the Maximum Password Age to Expires in **30** Days.
   - Configure the Minimum Password Age to Allow Changes in **5** Days.
   - Configure the Minimum Password Length to be At Least **8** Characters.
   - Configure Password Uniqueness to Remember (the last) **6** Passwords.
   - Select the radio button next to Account lockout.
   - Set Lockout after **3** bad logon attempts.
   - Set Reset count after **30** minutes.
   - Configure Lockout Duration to Forever (until admin unlocks).
   - Select the check box next to Users must log on in order to change password.

   Figure 8-9 shows the Account Policy dialog box as correctly configured at the close of this step. You can check the configurations you have made against this figure. Click OK.

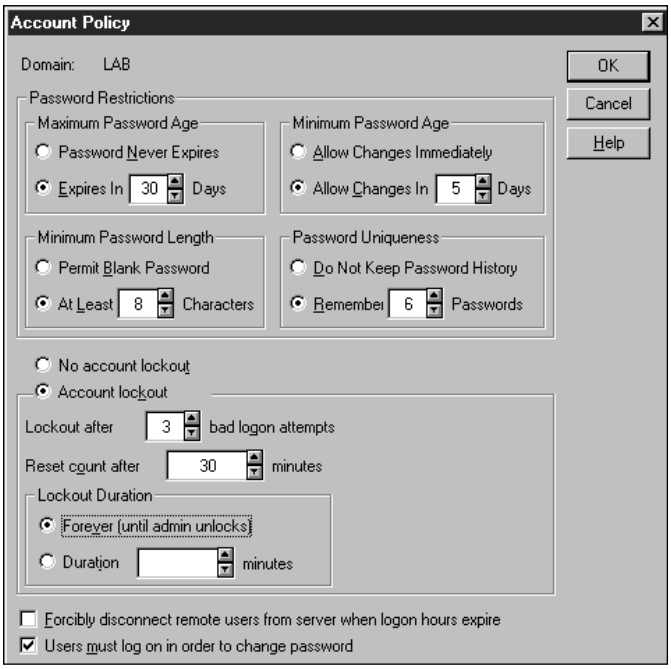


FIGURE 8-9 Account Policy dialog box as correctly configured in Lab 8.12

4. In the User Manager dialog box, select Policies ≥ User Rights.
5. The User Rights Policy dialog box appears. In the Right drop-down list box, select Log on locally. Click the Add command button.
6. The Add Users and Groups dialog box appears. In the Names list box, double-click the Everyone group. (Everyone appears in the Add Names list box.) Click OK. (Granting the "Log on locally" right to the Everyone group enables all users to log on interactively at the Windows NT Server.)
7. In the Users Rights Policy dialog box, click OK.
8. Exit User Manager.
9. Select Start ≥ Shut Down. In the Shut Down Windows dialog box, select the radio button next to Close all programs and log on as a different user. Click the Yes command button.
10. Press Ctrl + Alt + Delete to log on.
11. In the Logon Information dialog box, type in a user name of **JohnS** and a password of **newuser**. Click OK.
12. A dialog box appears, indicating you are required to change your password at first logon. (You may recall you set this configuration when you created this user in Lab 7.10.) Click OK.

13. The Change Password dialog box appears. Type in a new password of **password**. Confirm the new password by retyping it. Click OK.
14. A warning message appears, indicating you do not have permission to change your password. (This is because in the Account Policy dialog box you selected the check box next to "Users must log on in order to change password" *and*, when you created this user, you selected the option for User Must Change Password at Next Logon. *These two options do not work together*.) Click OK.
15. The Change Password dialog box appears. Click the Cancel command button.
16. The Logon Information dialog box appears. Type in a user name of **PamR** and a password of **wrongo**. Click OK. (Note: In this part of the lab you will attempt to log PamR on several times with an incorrect password to experience the account lockout feature.)
17. A warning message appears, indicating the system could not log you on. Click OK.
18. Repeat Steps 16 and 17 until a warning message appears, indicating NT is unable to log you on because your account has been locked out. You must contact your network administrator to unlock your account. Click OK. (Next, you will log on as administrator and unlock PamR's user account.)
19. In the Logon Information dialog box, type in a user name of **Administrator** and a password of **password**. Click OK.
20. Select Start ≥ Programs ≥ Administrative Tools (Common) ≥ User Manager for Domains.
21. In the User Manager dialog box, double-click the user account PamR in the Username list box.
22. The User Properties dialog box appears. Notice the check box next to Account Locked Out is checked. Deselect this check box. Click OK.
23. Double-click PamR again in the Username list box.
24. The User Properties dialog box appears. Notice the check box next to Account Locked Out is cleared and grayed out. (The Administrator can't lock out a user account — only the system can.) Click the Cancel command button.
25. In the User Manager dialog box, select Policies ≥ Account.
26. In the Account Policy dialog box, deselect the check box next to "Users must log on in order to change password." (This will enable users to change their passwords during logon.) Click OK.
27. Continue to Part 2.

Part 2: Creating users and configuring user rights

In this section you create two special-use user accounts and configure user rights for these new user accounts.

1. In the User Manager dialog box, select User ≥ New User.
2. The New User dialog box appears. Type the following bolded text in the appropriate text boxes:

   User name: **Admin2**

   Full name: **Administrator's Helper**

   Description: **User account with limited admin privileges**

   Password: **password**

   Confirm password: **password**

   Deselect the check box next to User Must Change Password at Next Logon. Select the check box next to Password Never Expires. Click the Add command button.
3. The New User dialog box reappears. Type the following bolded text in the appropriate text boxes:

   User name: **Backuponly**

   Full name: **Backup Operator's Helper**

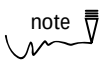
   Description: **Only able to back up files, not restore**

   Password: **password**

   Confirm password: **password**

   Deselect the check box next to User Must Change Password at Next Logon. Select the check box next to Password Never Expires. Click the Add command button. Click the Close command button.
4. In the User Manager dialog box, select Policies ≥ User Rights.
5. The User Rights Policy dialog box appears. In the Right drop-down list box, select "Log on locally." Click the Add command button.
6. The Add Users and Groups dialog box appears. Click the Show Users command button. Double-click Backuponly. Click OK.
7. In the Right drop-down list box, select Back up files and directories. Click the Add command button.
8. The Add Users and Groups dialog box appears. Click the Show Users command button. Scroll down and double-click Backuponly. Click OK. (The Backuponly user is now able to log on to the Windows NT Server and is able to back up the server's files.)

9. The User Rights Policy dialog box reappears. Using the sequence you used in the previous Steps 7 and 8, grant the following rights to the Admin2 user:
   - Add workstations to domain
   - Back up files and directories
   - Change the system time
   - Log on locally
   - Manage auditing and security log
   - Restore files and directories
   - Shut down the system
   - Take ownership of files or other objects



Note: You must go through all the steps for each user right you want to assign. No short cuts exist here.

Click OK in the User Rights Policy dialog box when you finish.

10. Exit User Manager for Domains. Continue to Part 3.

Part 3: Auditing revisited — clearing the security log in Event Viewer

In this section you explore the capabilities of the "Manage auditing and security log" user right, and clear the security log in Event Viewer.

1. Press Ctrl + Alt + Delete. Click the Logoff command button. Click OK to close all programs and log off.
2. Press Ctrl + Alt + Delete. In The Logon Information dialog box, type in a user name of **Admin2** and a password of **password**. Click OK. (If a Welcome to Windows NT screen is displayed, click the Close command button.)
3. Select Start ≥ Programs ≥ Administrative Tools (Common) ≥ User Manager for Domains.
4. In the User Manager dialog box, select Policies. Notice all the options in the Policies menu are grayed out. These options are only available to members of the Administrators group — The "Manage auditing and security log" user right does *not* give you the rights needed to set account policy, to configure user rights, or to enable auditing. Exit User Manager for Domains.
5. Select Start ≥ Programs ≥ Administrative Tools (Common) ≥ Event Viewer.
6. In the Event Viewer dialog box, select Log ≥ Security.
7. Select Log ≥ Clear All Events.

8. Click Yes in the Clear Event Log dialog box.
9. In the Save As dialog box, type **old security log** in the File name text box. Click the Save command button.
10. Click the Yes command button to clear the security log. The "Manage auditing and security log" user right authorizes a user to view and change the security log in Event Viewer, and enables a user to configure auditing of files, directories, and printers (in Windows NT Explorer, or in a printer's Properties dialog box, and so forth). But this user right does *not* enable a user to access the Audit Policy dialog box in User Manager or User Manager for Domains.
11. Exit Event Viewer.