

# MICROSOFT TRAINING AND CERTIFICATION

Administering Microsoft<sub>®</sub> Windows NT<sub>®</sub> 4.0

Student Workbook

Course Number: 803B

Part Number: X03-80309 Released: 02/99 Microsoft<sup>®</sup>

Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 1996, 1999 Microsoft Corporation. All rights reserved.

Microsoft, BackOffice, MS-DOS, MSN, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Susan Greenberg

Instructional Designers: Sandra Alto, Susan Stevenson, and Kathryn Yusi

Subject Matter Experts: Ryan Calafato and Rick Wallace

Technical Contributors: Kelley Beverly, Wally Mead, and Ken Rosen

Graphic Artist: Kimberly Jackson Graphic Contributors: Julie Stone

Editors: Pat Bezzio, Laurie Pritchard, and Marian Ranum, S&T OnSite Multimedia Producers: Susan Greenberg, and Beverly Hare, Media Solutions

Assistant Multimedia Producer: Sandra Alto

Interactive Lab Developer: Wendy Wahl, Madrona Software Production Support: Irene Barnett, Barnett Communications

Manufacturing Support: Bo Galford

Product Managers: Robert Stewart, Dean Murray, and Elaine Stovall

Multimedia Development: Digital Post & Graphics Web page development: Kate Knight, The Write Stuff

Course Number: 803B Part Number: X03-80309 Released: 02/99

## Contents

About This Course	
Course Overview	ix
Course Flow	xi
Document Conventions	xii
Introduction	
Introductions	3
Course Materials	4
Prerequisites	5
Course Outline	6
Microsoft Certified Professional Program	9
MCSE Track	11
Facilities	13
Classroom Configuration	14
Module 1: Introduction to Administering Windows NT	
Overview	
Administering Windows NT	18
Windows NT Administrative Tools	19
Logging On to a Computer or Domain	
The Windows NT Security Dialog Box	21
Review	22
Module 2: Setting Up User Accounts	
Overview	25
Introduction to User Accounts	26
Video: Overview of Windows NT Directory Services	27
Where Accounts Are Created	28
Planning New User Accounts	29
Naming Conventions	30
Passwords, Logon Hours, and Workstation Restrictions	31
Home Folder Location	32
Creating User Accounts	
Setting Password and Account Options	34
Setting Logon Hours	35
Setting Workstation and Account Options	36
Granting Dial-in Permission	37
Deleting and Renaming User Accounts	38
Lab 1: Planning and Creating User Accounts	39
Managing the User Work Environment	40
Roaming User Profiles	41
Creating Roaming User Profiles	42
Defining a User's Environment	43
Best Practices	44
Lab 2: Configuring User Profiles	45
Review	46

Module 3: Setting Up Group Accounts	
Overview	
Introduction to Groups	52
Video: Local and Global Groups	
Local and Global Groups Summary	54
Example of Using Local and Global Groups	55
Planning a Group Strategy	56
Creating Local and Global Groups	57
Creating Global Groups	58
Creating Local Groups	59
Deleting Groups	60
Lab 3: Planning and Creating Local and Global Groups	61
Implementing Built-in Groups	62
Built-in Groups on All Windows NT-Based Computers	63
Built-in Groups on Domain Controllers Only	64
Built-in System Groups	65
Best Practices	66
Lab 4: Implementing Built-in Groups	67
Review	68
Module 4: Administering User and Group Accounts	
Overview	
Introduction to Administering Accounts	74
Creating User Account Templates	
Using Templates to Create User Accounts	76
Implementing an Account Policy	77
Planning an Account Policy	78
Setting Password Options	80
Setting Account Lockout Options	81
Resetting User Account Passwords	82
Unlocking User Accounts	
Modifying Multiple User Accounts	84
Lab 5: Managing Accounts	85
Maintaining Domain Controllers	86
Promoting a Backup Domain Controller	87
Resuming Domain Controller Roles	88
Synchronizing Domain Controllers	89
Troubleshooting Logon Problems	90
Lab 6: Managing Domain Controllers	91
Review	92
Module 5: Securing Network Resources with Shared Folder Permissions	
Overview	
Introduction to Shared Folders	
Shared Folder Permissions	. 97
How User and Group Permissions Are Applied	. 98
Examples of Applied Permissions	. 99

Guidelines for Sharing Folders	
Examples of Shared Folders	
Guidelines for Assigning Permissions	
Guidelines for Network Application Folders	
Guidelines for Data Folders	
Guidelines for Home Folders	
Lab 7: Planning Shared Folders	
Sharing Folders	
Sharing a Folder	108
Assigning Shared Folder Permissions	109
Modifying Shared Folders	110
Accessing Shared Folders	111
Best Practices	
Lab 8: Sharing Folders	114
Review	
Module 6: Securing Network Resources with NTFS Permissions	
Overview	119
Introduction to NTFS Permissions	120
NTFS Permissions	121
Standard Permissions	122
How NTFS Permissions Are Applied	123
Combining Shared Folder and NTFS Permissions	
Video: Permissions	
Examples of Combining NTFS and Shared Folder Permissions	
Guidelines for Assigning NTFS Permissions	
Home Folders	128
Assigning NTFS Permissions	129
Assigning NTFS File and Folder Permissions	130
Assigning Special Access Permissions	131
Lab 9: Planning and Assigning NTFS Permissions	132
Taking Ownership of Folders and Files	133
Copying or Moving Folders and Files	134
Examples of Copying and Moving Folders and Files	135
Troubleshooting Permission Problems	136
Best Practices	
Lab 10: Managing Permissions	139
Review	140
Module 7: Setting Up a Network Printer	
Overview	
Introduction to Windows NT Printing	144
Printer Permissions	
Setting Up a Network Printer	146
Adding and Sharing a New Printer	
Sharing an Existing Printer	
Assigning Printer Permissions	150
Setting Up a Network Client	

Accessing a Network Printer	152
Creating a Printing Pool	154
Setting Priorities Between Printers	155
Scheduling Documents	156
Assigning Forms to Paper Trays	158
Setting a Separator Page	159
Best Practices	160
Lab 11: Setting Up a Network Printer	161
Review	162
Module 8: Administering Network Printers	
Overview	165
Introduction to Administering Printers	166
How Documents Print	
Deleting a Document	168
Setting a Notification, Priority, and Printing Time	169
Pausing, Resuming, and Purging a Printer	170
Redirecting Documents	
Taking Ownership of a Printer	
Identifying Printing Problems	
Lab 12: Managing Documents and Printers	
Review	
Module 9: Auditing Resources and Events	
Overview	179
Introduction to Auditing	180
Planning an Audit Policy	
Implementing an Audit Policy	
Defining an Audit Policy	
Auditing Files and Directories	
Auditing a Printer	
Using Event Viewer	
Viewing Security Logs	
Locating Events	
Archiving the Security Log	
Best Practices	
Lab 13: Auditing Resources and Events	
Review	
Module 10: Monitoring Network Resources	
Overview	197
Introduction to Monitoring Network Resources	198
Monitoring Computer Properties	
Monitoring User Sessions	
Monitoring Shared Resources	
Monitoring Resources in Use	
Setting Administrative Alerts	
Sending Messages to Users	

Viewing a System Configuration	206
Best Practices	208
Lab 14: Monitoring Network Resources	209
Review	210
Module 11: Backing Up and Restoring Data	
Overview	213
Introduction to the Windows NT Backup Program	214
Planning a Backup Strategy	215
Determining Which Files and Folders to Back Up	
Determining the Backup Type to Use	
Examples of Using Different Backup Types	219
Rotating and Archiving Tapes	220
Backup Sets, Catalogs, and Backup Logs	
Backing Up Data	
Selecting Drives, Files, and Folders	223
Setting Tape and Backup Options	
Setting Log Options	226
Scheduling a Backup Using a Batch File	227
Example of a Scheduled Backup	229
Using the At Command	
Lab 15: Backing Up Data to Tape	232
Implementing a Restore Strategy	233
Examples of Restore Strategies	234
Restoring Data	235
Catalogs	236
Selecting Backup Sets, Files, and Folders	237
Selecting Restore Options	238
Selecting Log Options	239
Best Practices	
Lab 16: Restoring Data from Tape	
Review	242

## **About This Course**

#### **Course Overview**

#### **Description**

This course provides you with the knowledge and skills necessary to perform post-installation and day-to-day administration tasks in a single-domain or multiple-domain Windows NT<sub>®</sub>-based network. It also provides you with the prerequisite knowledge and skills required for course 687, *Supporting Microsoft Windows NT 4.0 Core Technologies*.

This course is intended for those who administer Windows NT Server and Windows NT Workstation, or for those who are on the Microsoft Certified Systems Engineer (MCSE) Windows NT 4.0 track.

#### **Prerequisites**

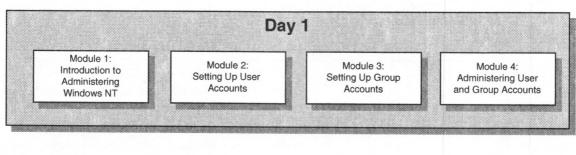
- Working knowledge of the Microsoft Windows 95 or Windows NT 4.0 interface, including the ability to:
  - Use Windows Explorer
  - Start an application
  - Open, close, minimize, maximize, and move windows
  - Switch between applications and tasks
- Knowledge of basic computer hardware components, including computer memory, hard disks, central processing unit (CPU), communication and printer ports, display adapters, and pointing devices
- Knowledge of major networking concepts, including client, server, local area network (LAN), wide area network (WAN), network adapter card, driver, protocol, and network operating system

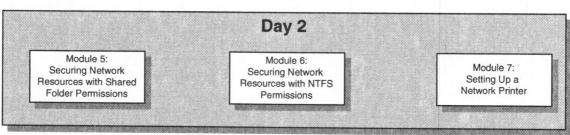
#### **Objectives**

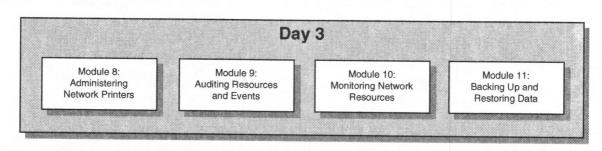
At the end of this course, you will be able to:

- Create and administer user and group accounts, including the ability to:
  - Plan user accounts.
  - Define the user environment.
  - Create user profiles.
  - Implement an account policy.
  - · Manage domain controllers.
  - Troubleshoot logon problems.
- Manage disk resources, including the ability to:
  - Plan how resources are shared.
  - Set up and administer permissions for files and folders.
  - · Take ownership of files and folders.
  - Troubleshoot when users are unable to gain access to disk resources.
- Set up and administer a network printer, including solving common printing problems.
- Define an audit policy and set up file, directory, and printer auditing.
- Monitor server resources to track usage and disk space.
- Back up and restore files and directories using tapes.

## **Course Flow**







## **Document Conventions**

The following conventions are used in course materials to distinguish elements of the text.

Convention	Use
•	Indicates an overview or introductory page. This symbol appears next to a slide title when additional information on the topic is covered on the page or pages that follow it.
bold	Represents commands, command options, and portions of syntax that must be typed exactly as shown. It also indicates commands on menus and buttons, dialog box titles and options, and menu names.
italic	In syntax statements, indicates placeholders for variable information. Italic is also used for important new terms, for book titles, and for emphasis in the text.
Title Capitals	Indicate directory names, file names, and folders (except when specifically referring to case-sensitive names).  Unless otherwise indicated, you can use lowercase letters when you type a directory name or file name in a dialog box or at the command prompt.
SMALL CAPITALS	Indicate the names of keys, key sequences, and key combinations—for example, ALT+SPACEBAR.
monospace	Represents code samples and examples of screen text.
[]	In syntax statements, enclose optional items. For example, [filename] in command syntax indicates that you can choose to type a file name with the command. Type only the information within the brackets, not the brackets themselves.
{}	In syntax statements, enclose required items. Type only the information within the braces, not the braces themselves.
1	In syntax statements, separates an either/or choice.
<b>&gt;</b>	Indicates a procedure with sequential steps.
	In syntax statements, specifies that the preceding item may be repeated.
	Represents an omitted portion of a code sample.

## Introduction

## Introductions

- **Name**
- **Company Affiliation**
- **Title/Function**
- **■** Job Responsibility
- Networking Experience
- **Microsoft® Windows NT® Experience**
- **Expectations**

## **Course Materials**

- Name Card
- **™ Student Workbook**
- **Lab Manual**
- **Compact Disc**
- **Course Evaluation**
- **Reference Materials**

Write your name on both sides of the name card so that students in front of you and in back of you will know who you are.

#### **Student Workbook**

The student workbook contains the slide graphics and text covered during lectures. This workbook is yours to keep.

#### Lab Manual

The lab manual contains the hands-on lab exercises and lab answers used during class. This manual is yours to keep.

#### **Compact Disc**

The compact disc contains supplemental material for the course, including all the lab files and video clips used throughout the class. It also contains additional resources for continued learning.

#### **Course Evaluation**

Before class is over, please complete the course evaluation to provide feedback on the instructor, course, and software product. Your comments will help us improve future courses.

#### **Reference Materials**

Reference materials, such as product documentation, are for classroom use only.

**Note** No video or audio recordings are permitted.

## **Prerequisites**

- Working Knowledge of Windows 95 or Windows NT 4.0 Interface
- **Knowledge of Basic Computer Hardware Components** 
  - RAM, hard disks, CPU, printer ports
- Knowledge of Basic Networking Concepts
  - Local area network (LAN) / wide area network (WAN)
  - Network operating system
  - Network adapter card
  - Driver and protocol

### **Course Outline**

- **Module 1: Introduction to Administering Windows NT**
- Module 2: Setting Up User Accounts
- **Module 3: Setting Up Group Accounts**
- Module 4: Administering User and Group Accounts
- Module 5: Securing Network Resources with Shared Folder Permissions
- Module 6: Securing Network Resources with NTFS Permissions

Module 1, "Introduction to Administering Windows NT," introduces Microsoft® Windows NT® administration and tools, the basics required to log on to a computer in a network environment, and how to use the **Windows NT Security** dialog box.

Module 2, "Setting Up User Accounts," provides instruction on the types of user accounts, considerations for planning new user accounts, and how to create user accounts. A video on directory services provides an overview of a Windows NT environment and the role user accounts play in it. The rest of the module presents tasks related to managing the user work environment, including creating a roaming mandatory user profile. Procedures for renaming and deleting accounts are also included. At the end of this module, you will be able to plan and create user accounts.

Module 3, "Setting Up Group Accounts," provides an introduction to local and global groups in Windows NT, a planning strategy for implementing groups in a domain, procedures for creating local and global groups, and a description of built-in groups and how to implement them. At the end of this module, you will be able to plan and create group accounts.

Module 4, "Administering User and Group Accounts," presents a selection of tasks related to administering accounts. You will learn how to copy a user account to create a new one, how to create user account templates, how to plan and implement an account policy, how to make a modification to many user accounts at one time, and how to solve problems related to user accounts. You will also learn procedures for managing domain controllers. At the end of this module, you will be able to perform various tasks related to account administration.

Module 5, "Securing Network Resources with Shared Folder Permissions," introduces the concepts of shared folders and related permissions and how permissions are applied, and what guidelines to use for sharing folders and assigning permissions. It includes procedures for sharing folders and assigning permissions, modifying a shared folder, and connecting to a shared folder over the network. At the end of this module, you will be able plan and create shared folders, and assign permissions to those folders.

Module 6, "Securing Network Resources with NTFS Permissions," provides instruction on how NTFS permissions are applied, how to combine shared folder permissions and NTFS permissions, and how to assign NTFS file and folder permissions. You will also learn how to customize permissions; how to take ownership, copy, and move folders and files; and how to troubleshoot various permission problems. At the end of this module, you will be able to assign NTFS file and folder permissions, and perform some permissions troubleshooting.

## **Course Outline** (continued)

- Module 7: Setting Up a Network Printer
- **Module 8: Administering Network Printers**
- Module 9: Auditing Resources and Events
- Module 10: Monitoring Network Resources
- Module 11: Backing Up and Restoring Data

Module 7, "Setting Up a Network Printer," provides an introduction to printing using Windows NT, including guidelines and procedures for setting up a network printer and clients, sharing a printer, and assigning permissions, creating a printing pool, and setting priorities. At the end of this module, you will be able to set up a network printer.

Module 8, "Administering Network Printers," provides instruction on tasks related to managing documents, such as pausing and resuming printing, managing printers, taking ownership of a printer, and identifying printing problems. At the end of this module, you will be able to administer network printers.

Module 9, "Auditing Resources and Events," provides instruction on auditing, including how to plan and implement an audit policy, how to set up auditing on files and printers, and how to use Event Viewer. At the end of this module, you will be able to audit and archive resources and events.

Module 10, "Monitoring Network Resources," provides an overview of using Server Manager to view computer properties, monitor user sessions, shared resources, and resources in use, set administrative alerts, and send messages to users. It also covers how to use Windows NT Diagnostics to view hardware and system configuration information. At the end of this module, you will be able to monitor computer properties and view system configuration.

Module 11, "Backing Up and Restoring Data," provides instruction in tasks related to backing up and restoring data, including guidelines for planning a backup strategy and the procedures for backing up data; determining the backup type to use; how and when to rotate and archive tapes; what the differences are between backup sets, logs, and catalogs; plans for a backup schedule; and procedures for backing up and restoring data. At the end of this module, you will be able to back up and restore data.

## Microsoft Certified Professional Program

- **Microsoft Certified Systems Engineer (MCSE)**
- **Microsoft Certified Solution Developer (MCSD)**
- Microsoft Certified Product Specialist (MCPS)
- **Microsoft Certified Trainer (MCT)**



The Microsoft Certified Professional (MCP) program provides the best method to prove your command of current Microsoft products and technologies. Anyone who must prove his or her technical expertise with Microsoft products should consider the program, including systems engineers, product developers, support technicians, system and network administrators, consultants, and trainers.

The following table describes the four certifications, based on specific areas of technical expertise.

Certification	Description
Microsoft Certified Systems Engineer (MCSE)	MCSEs are qualified to effectively plan, implement, maintain, and support information systems in a wide range of computing environments with Windows NT Server and the Microsoft BackOffice™ integrated family of server products.
Microsoft Certified Solution Developer (MCSD)	MCSDs are qualified to design and develop custom business solutions with Microsoft development tools, technologies, and platforms, including Microsoft Office and Microsoft BackOffice.
Microsoft Certified Product Specialist (MCPS)	MCPSs demonstrate in-depth knowledge of at least one Microsoft operating system. Candidates may pass additional Microsoft certification exams to further qualify their skills with Microsoft BackOffice products, development tools, or desktop applications.
Microsoft Certified Trainer (MCT)	MCTs are instructionally and technically qualified to deliver Microsoft Official Curriculum through Microsoft Authorized Technical Education Centers.

#### Requirements

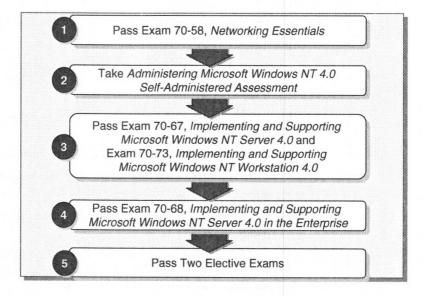
The certification requirements differ for each certification and are specific to the products and job functions addressed by the certification. To become a Microsoft Certified Professional, you must pass rigorous certification exams that provide a valid and reliable measure of technical proficiency and expertise.

The following table describes exam requirements.

Certification	Exam requirements
Microsoft Certified Systems Engineer (MCSE)	Pass a series of operating system exams and elective exams.
Microsoft Certified Solution Developer (MCSD)	Pass two core technology exams and two elective exams.
Microsoft Certified Product Specialist (MCPS)	Pass one operating system exam. In addition, individuals seeking to validate their expertise in a program must pass the appropriate elective exam.
Microsoft Certified Trainer (MCT)	Required to meet instructional and technical requirements specific to each Microsoft Official Curriculum course they are certified to deliver.

<sup>&</sup>lt;sup>1</sup> Inside the United States and Canada call (800) 636-7544 for more information on becoming a Microsoft Certified Trainer. Outside the United States and Canada, contact your local Microsoft subsidiary.

#### **MCSE Track**



The following table outlines the recommended path to certification.

Step	Pass this exam	Preparation
1	70-58, Networking Essentials	Course 683, Networking Essentials— Self-paced Training Kit
2	Administering Microsoft Windows NT 4.0 self-administered assessment	Course 803, Administering Microsoft Windows NT 4.0
3	70-67, Implementing and Supporting Microsoft Windows NT Server 4.0 and exam 70-73, Implementing and Supporting Microsoft Windows NT Workstation 4.0 <sup>2</sup>	Course 687, Supporting Windows NT Core Technologies
4	70-68, Implementing and Supporting Microsoft Windows NT Server 4.0 in the Enterprise	Course 689, Supporting Windows NT Server 4.0 Enterprise Technologies
5	Two elective exams (from the following list)	

<sup>&</sup>lt;sup>2</sup> Exam 70-73, *Implementing and Supporting Microsoft Windows NT Workstation 4.0* can be substituted by another client exam. For a complete list of client exams, see the Microsoft Training and Certification Web site at http://www.microsoft.com/train\_cert

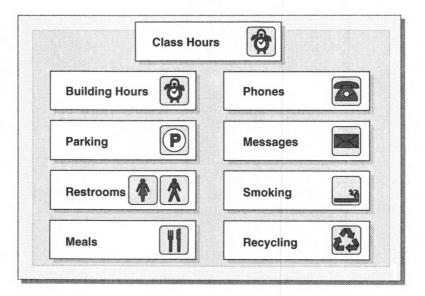
#### **Elective Exams**

Pass any two of the following exams to complete the certification track:

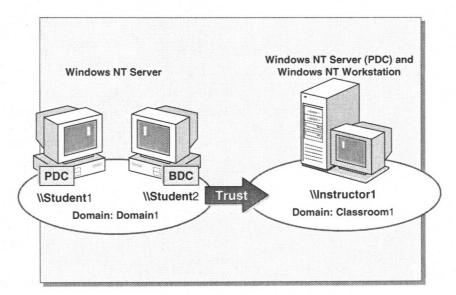
- 71-75, Implementing and Supporting Microsoft Exchange Server 4.0
- 70-27, Implementing a Database Design on Microsoft SQL Server 6
- 70-26, System Administration of Microsoft SQL Server 6
- 70-12, Microsoft SNA Server
- 70-53, Internetworking Microsoft TCP/IP on Microsoft Windows NT (3.5-3.51)
- 70-21, Microsoft SQL Server 4.2 Database Implementation
- 70-14, Implementing and Supporting Microsoft Systems Management Server 1.0
- 70-22, Microsoft SQL Server 4.2 Database Administration for Microsoft Windows NT
- 70-26, System Administration for Microsoft SQL Server 6 or Exam 70-22, Microsoft SQL Server 4.2 Database Administration for Microsoft Windows NT
- 70-27, Implementing a Database Design on Microsoft SQL Server 6 or 70-21 Microsoft SQL Server 4.2 Database Implementation
- 70-37, Microsoft Mail 3.2 for PC Networks—Enterprise

**For More Information** See the Certification section of the Web page provided on the Supplemental Material compact disc. To open the Web page, in the \WebDocs directory, double-click **open.htm**.

## **Facilities**



## **Classroom Configuration**



The following configuration and naming conventions are used throughout the course and are required for the hands-on labs:

- The instructor's computer is configured with Windows NT Workstation and Windows NT Server as a primary domain controller (PDC).
  - The computer name is \\Instructorx (where x is a unique number).
  - This computer is in the domain named Classroomx (where x is a unique number).
- All student computers are configured with Windows NT Server only.
  - Each computer is named Studentx (where x is the assigned student number).
  - Every two computers are in a domain named Domainx (where x is a unique number). This domain is set up to *trust* the Classroomx domain.
  - One computer in the domain is configured as a Windows NT Server PDC, and the other computer is configured as a Windows NT Server backup domain controller (BDC).

**Note** Domain concepts will be discussed in more detail throughout the course.

# Module 1: Introduction to Administering Windows NT

## Overview

- Administering Windows NT
- Windows NT Administrative Tools
- Logging On to a Computer or Domain
- The Windows NT Security Dialog Box

#### **Objectives**

At the end of this module, you will be able to:

- Describe the tasks required for administering Microsoft® Windows NT® Workstation and Windows NT Server.
- Log on to a computer or domain.
- Describe the functions of the Windows NT administrative tools for Windows NT Server and Windows NT Workstation.
- Lock a workstation, change a password, switch between tasks, log off, and shut down the computer.
- Use online Help to locate information.

**Note** Information provided in this course applies to both Windows NT Workstation and Windows NT Server unless otherwise noted.

## **Administering Windows NT**

#### Windows NT Administration Includes:

- Post-installation tasks
- Day-to-day tasks

#### **■ The Five Categories of Tasks Include:**

- User and group account administration
- Printer administration
- Security administration
- Monitoring network events and resources
- Backing up and restoring data

Administering Windows NT involves post-installation and day-to-day tasks required for Windows NT Workstation and Windows NT Server. The administration tasks can be grouped into five general categories.

This category	Includes these tasks
User and group account administration	Planning, creating, and maintaining user and group accounts to ensure that each user can log on to the network and access necessary resources.
Printer administration	Setting up local and network printers and troubleshooting common printing problems. This ensures that users can connect to and use printer resources easily.
Security administration	Planning, implementing, and enforcing a security policy for protecting data and shared network resources, including folders, files, and printers.
Monitoring network events and resources	Planning and implementing a policy for tracking security breaches, and monitoring and controlling resource usage.
Backing up and restoring data	Planning, scheduling, and performing regular backups to protect important data. Having a good backup plan ensures that you can quickly locate and restore critical data.

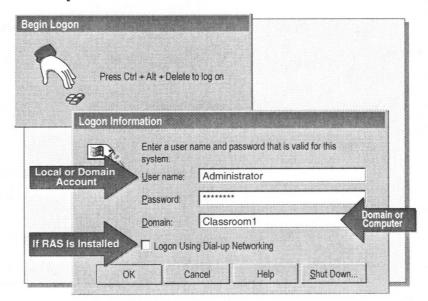
## **Windows NT Administrative Tools**

- Windows NT Server Only (DOTGEN CONTROLER)
  - Administrative Wizards
  - Server Manager
  - User Manager for Domains
- **™** Windows NT Workstation Only
  - User Manager
- **Windows NT Server and Windows NT Workstation** 
  - Backup
  - Event Viewer
  - Windows NT Diagnostics
  - Help

The following tables describe the Windows NT tools useful for network administration.

Windows NT Server	Purpose
Administrative Wizards	Steps you through administrative tasks, such as creating user accounts, creating and modifying group accounts, setting permissions on files and folders, and setting up network printers.
Server Manager	Views and manages domains and computers.
User Manager for Domains	Manages security for domains, member servers, and workstations. If the computer is not configured as a domain controller, User Manager is installed.
Windows NT Workstation	Purpose
User Manager	Manages security for computers running Windows NT Workstation.
Both operating systems	Purpose
Backup	Backs up data to protect it from accidental loss or hardware and media failures.
Event Viewer	Monitors events in a computer. Event Viewer provides information about errors, warnings, and success or failure of a task, such as user logon attempts.
Windows NT Diagnostics	Views and prints system configuration information, such as information about memory, drives, and services.

## Logging On to a Computer or Domain

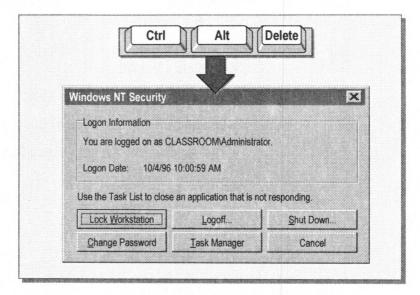


Each time you start the computer, Windows NT prompts you to log on by pressing CTRL+ALT+DELETE. The **Logon Information** dialog box is used to log on to a computer or domain.

The following table describes the dialog box options.

Option	Description
User name	Enter the unique user account that was assigned by an administrator. To log on to a domain, this account must reside in the directory database on domain controllers. To log on to a computer, this account must reside in the directory database of the local computer.
Password	Enter the password assigned to the user name. Passwords are case- sensitive. The password appears as asterisks to protect it from onlookers.
Domain	To log on to the domain, select the name of the domain. If you log on to the domain, the domain controller's directory database is checked and validates the account.
	To log on to a computer, select the name of the computer. If you log on to the local computer, the local computer's directory database is checked and validates the account.
	A user can <i>only</i> log on to a computer with a user name that resides in the local computer's directory database. Member servers and computers running Windows NT Workstation have a local Administrator and Guest account by default. Other local accounts must be created.
Logon Using Dial-up Networking	When the Remote Access Service (RAS) is installed, selecting this check box allows a user to log on to a remote network using RAS.
Shut Down	Closes all files, saves all operating system data, and prepares the computer to be safely turned off. On Windows NT Server, this button is disabled to prevent an unauthorized user from shutting down the server.

## The Windows NT Security Dialog Box



Once a user is logged on, the CTRL+ALT+DELETE key sequence is used to access the **Windows NT Security** dialog box. The following table describes the dialog box options.

Option	Function
Lock Workstation	Secures the computer without logging off. All applications remain running.
	A locked workstation can only be unlocked by the current user or an administrator. If an administrator unlocks it, the only thing the administrator can do is log the user off.
Change Password	Allows a user to change the user account password. The user must know the old password before a new one can be created. This prevents users from changing other user's passwords. This is the only way for users to change their passwords.
Logoff	Logs off the current user, but leaves Windows NT services running. Always log off when you no longer need to use computer.
Task Manager	Lists the current applications that are running. Task Manager is used to switch between applications, and to stop an application that is not responding.
Shut Down	Closes all files, saves all operating system data, and prepares the server to be safely turned off.
Cancel	Closes the Windows NT Security dialog box.

### Review

- Administering Windows NT
- **Windows NT Administrative Tools**
- **Logging On to a Computer or Domain**
- The Windows NT Security Dialog Box

- 2. What key sequence is used to log on to a computer or domain and to access the **Windows NT Security** dialog box?

- 3. From which dialog box do users change their passwords? NT SECRITY DIALOG ROX
- 4. How can users secure their computers without logging off?
- 5. What should users always do before they turn off a computer running Windows NT?

## Module 2: Setting Up User Accounts

## Overview

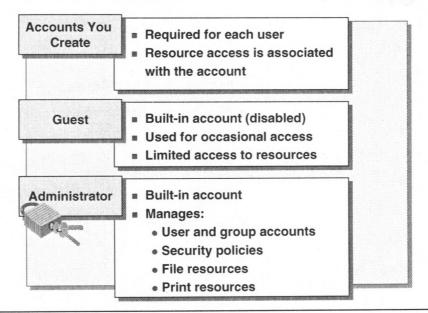
- **Introduction to User Accounts**
- **Planning New User Accounts**
- **Creating User Accounts**
- **Deleting and Renaming User Accounts**
- Managing the User Work Environment
- **Best Practices**

#### **Objectives**

At the end of this module, you will be able to:

- Describe the types of user accounts.
- Describe the Microsoft® Windows NT® directory services and the role user accounts play in them.
- Describe the function of primary and backup domain controllers and member servers.
- Describe the difference between a domain user account and a local user account.
- Plan a strategy for creating new user accounts.
- Create new user accounts, including home folders.
- Delete and rename user accounts.
- Change a user's working environment.
- Apply best practices for creating user accounts.

## **◆** Introduction to User Accounts



#### What Is a User Account?

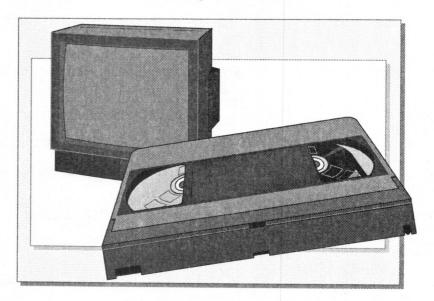
A user account is a user's unique credentials and gives the user the ability to log on to the domain to access network resources, or to log on to a local computer to access local resources. Each person who regularly uses the network should have an account. You use user accounts to control how a user accesses the domain or a computer. For example, you can limit the number of hours a user can log on to the domain.

#### **Types of User Accounts**

There are two types of user accounts, accounts you create and built-in accounts. The following table describes the types of user accounts.

Account	Description
Accounts you create	These user accounts enable the user to log on to the network and, with the appropriate permissions, to access network resources. These accounts contain information about the user, including the user's name and password.
Guest	The built-in Guest account is used to give occasional users the ability to log on and access resources on the local computer. For example, an employee that needs to access the computer for a short time can use the Guest account. The Guest account is disabled by default.
Administrator	The built-in Administrator account is used to manage the overall computer and domain configuration. The Administrator account can be used to perform all tasks, such as creating, or modifying, user and group accounts; managing security policies, creating printers, and assigning permissions and rights to user accounts to access resources.

## **Video: Overview of Windows NT Directory Services**



This video describes the Windows NT environment and the role of user accounts in Windows NT directory services. It also defines key terminology that will be used throughout this course.

As you view the video, look for the answers to following questions:

- 1. What three things are provided by Windows NT Server directory services?

  Single user logar, Universial access to , Remote access (contralised administral)
- 2. What are the three Windows NT Server configurations?
- 3. How many primary domain controllers can there be in each domain? How many backup domain controllers?

  or number or pero.
- 4. How does a domain differ from a peer-to-peer network?

  one Central DE DE Directory DE on each machine.
- 5. What is the logical link that combines domains into one administrative unit? t t

#### Where Accounts Are Created

- In the Master Directory Database on the PDC in a Domain
  - With User Manager for Domains
  - A copy of the directory database is stored on all BDCs
- In the Local Directory Database of the Local Computer
  - With User Manager on a member server or computer running Windows NT Workstation

#### **Domain User Account**

A domain user account is created with User Manager for Domains. When a user account is created in a domain, the user account is always created in the master directory database of the primary domain controller (PDC). A copy of the directory database is stored on all backup domain controllers (BDCs). Once the user account is created on the PDC, a user can log on to the domain from any computer in the network.

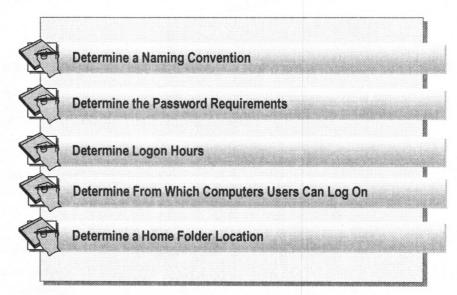
**Note** It may take a few minutes before the copies of the directory database on the BDCs are synchronized with the PDC; this may prevent users with new accounts from logging on. To manually synchronize the database on all domain controllers, use Server Manager, or at a command prompt, type **net accounts** /sync and then press ENTER.

#### **Local User Account**

Local user accounts are created on a member server or a computer running Microsoft Windows NT Workstation, with User Manager. When you create a local user account, the account is created *only* in that computer's local directory database. With a local user account, a user can log on to and access resources on only that computer.

**Note** You can create domain user accounts from computers running Windows NT Workstation and Microsoft Windows® 95 by installing the Windows NT Server Administrative Tools from the Windows NT Server compact disc.

# Planning New User Accounts



You can streamline the process of creating user accounts by planning and organizing the information for people who will need user accounts.

To plan user accounts you need to determine:

- A naming convention that ensures unique but consistent user account names. A consistent naming convention will make it easy for you and your users to remember user names and locate them in lists.
- Whether you or the user will determine the user account password to prevent unauthorized users from logging on to the network.
- The hours that users need to be able to access the network or be restricted from using the network.
- What computers users will be able to log on from to control what computers may be used to access network data.
- Whether home folders will be located on the local computer or on a server for centralized backup and administration.

### **Naming Conventions**

- User Account Names Must Be Unique
  - Domain accounts must be unique to the domain
  - Local accounts must be unique to the computer
- **User Accounts Can Contain Up to 20 Characters**
- Consider a Naming Convention that:
  - Accommodates duplicate employee names
  - Identifies temporary employees

Examples

Duplicate Names	Temporary Employees
BarbaraL or BarbaraLa BarbaraL1 or BarbaraL2	T-BarbaraL

The naming convention establishes how users will be identified on the network. A consistent naming convention will make it easy for you and your users to remember user names and locate them in lists.

To determine a naming convention, consider the following points:

- User names must be unique. Domain user accounts must be unique to the domain. Local user accounts must be unique to the local computer.
- User names can contain up to 20 uppercase or lowercase characters except for the following: " / \ [ ]:; | = , + \* ? < >. You can use a combination of special and alphanumeric characters in your naming convention to help identify users.
- If you have a large number of users, your naming convention should accommodate employees with duplicate names. Some suggestions for handling duplicate names are:
  - Use the first name and the last initial, and then add additional letters
    from the last name to accommodate duplicate names. For example, for
    two users named Barbara Lang, one user name could be BarbaraL and
    the other BarbaraLa.
  - Add numbers to the user name. For example, BarbaraL1 and BarbaraL2.
- In large organizations it is useful to identify temporary employees by their user account. For example, to identify temporary employees, use a "T" and a dash in front of the user name. For example, T-BarbaraL.

## Passwords, Logon Hours, and Workstation Restrictions

- Assign the Administrator Account a Password
- Set an Expiration on Temporary Employee Accounts

  not ease sensitive

   case sen
  - Educate Users on How to Protect Passwords
    - Avoid obvious associations, such as family and pet names
    - Use long passwords (up to 14 characters)
    - Use a combination of uppercase and lowercase characters
  - Set Logon Hours to a User's Work Hours
  - Require Users to Log On from Their Own Computers

### **Passwords**

To protect access to the domain or a computer, every user account requires a password. Consider the following guidelines for passwords:

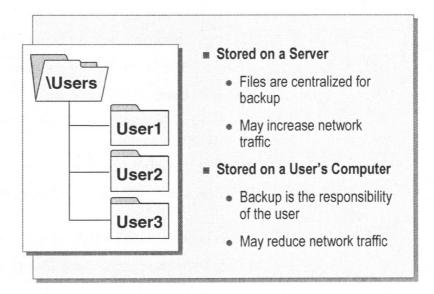
- Always assign the Administrator account a password to prevent unauthorized users from using the account.
- Determine who will control the password. You can either assign users unique passwords and prevent users from changing them, or you can allow users to enter their own passwords the first time they log on. In most networks, users should control their passwords.
- Determine whether an account needs to expire. You should set user accounts for temporary employees to expire when their contract ends.
- Educate users on ways to protect and enter their passwords:
  - Avoid using an obvious association, such as a family member's name.
  - Use long passwords. Passwords can be up to 14 characters in length.
  - Use both uppercase and lowercase letters. Passwords are case-sensitive. For example, the password *SeCret* is different from *secret*.

### **Logon Hours and Workstation Restrictions**

You should assess the hours a user can log on to the network, and from what computers a user can log on. To determine logon hours and workstation restrictions consider the following points:

- Logon hours should be set for users that only require access at specific time periods. For example, only allow night shift workers to log on during their working hours.
- Users should be required to log on from their own computers when sensitive data is stored on their local computers.

### **Home Folder Location**

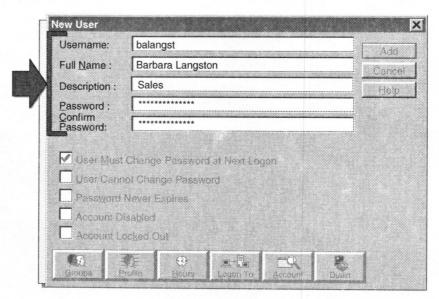


A home folder is a user's private folder for storing files. It is used as the default folder for the **File Open** and **Save As** dialog boxes, when the command prompt is started, and for opening or saving a file in programs that do not supply a default working folder.

A home folder can be stored on a user's local computer, or on a network server. Consider the following points when determining the home folder location:

- Backup and restore—preventing the loss of data is your primary responsibility. It is much easier to ensure files are backed up when they are located in a central location on a server. If users' home folders are located on their local computers, you would need to perform regular backups on each computer.
- Space on the domain controllers—is there enough room on the PDC or on the BDCs to allow users to store their data? Windows NT does not provide the ability to limit the amount of hard disk space used by each user.
- Space on the users' computers—if users are working on computers with very little disk space or no hard disks, home folders should be located on a network server.
- Performance—there is less network traffic if the home folder is located on the user's local computer.

# Creating User Accounts



User the following procedure to create a user account. The only requirement is to assign a user name.

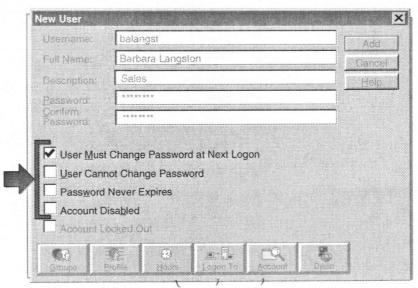
### ► To create a new user account

- Start User Manager for Domains (or User Manager on Windows NT Workstation).
- 2. On the User menu, click New User.
- 3. Configure the following options.

In this box	Туре
Username	A unique name based on your naming convention. This is required.
Full Name	The complete name of the user is helpful to determine which person belongs to an account. This is optional.
Description	A description that is useful in your environment for identifying users. It can be a job classification, a department, or an office location. This is optional.
Password	A password, but only if you will control the password for the account. You do not have to assign a password to an account; however, for greater security you should <i>always</i> make sure the user changes his or her password when he or she first logs on.
	Notice that the password is not displayed. It is represented by a series of fourteen asterisks once you enter the password, regardless of the length of the password.
Confirm Password	Type the password a second time to make sure that you typed the password correctly. This is required if a password is assigned.

4. Click **Add** and the user account is created. After you click **Add**, all of your entries disappear. This allows you to create another new user account.

# **Setting Password and Account Options**



in User Monger for Demain ONLY!

#### ► To set password and account options

Select or click to clear the following check boxes.

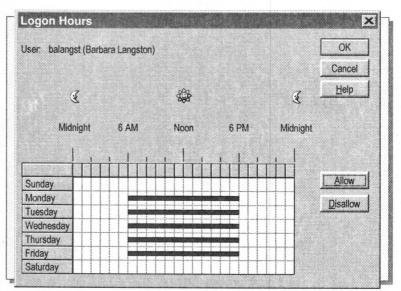
Select this check box	If you
User Must Change Password at Next Logon (selected by default)	Want users to change their password the first time that they log on. This ensures that the user is the only person who knows his or her password.
User Cannot Change Password	Have more than one person using the same user account, such as Guest, or want to maintain control over user passwords.
Password Never Expires	Have a user account for which you never want the password to change. For example, user accounts that will be used by services to log on (such as the Replicator service).
	This option overrides the selection of User Must Change Password at Next Logon.
Account Disabled	Want to temporarily prevent use of this account—for example, if an employee takes a leave of absence.
late an Account -> re-create w	leave of absence.  With same Name/Password > different

## **Setting Logon Hours**

default: logon enry

N.E. con continue using the machine if logan before restricted period.

RUT may have problem in accessing network resource during off-hours



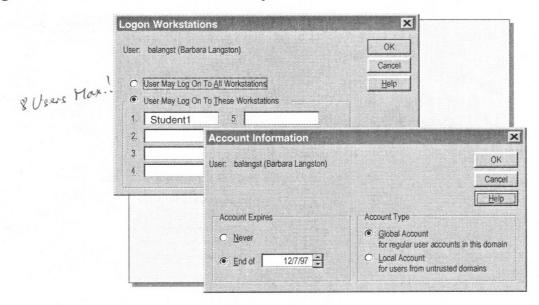
Setting logon hours lets you control when a user can log on to the domain. Restricting logon hours limits the hours that users can explore the network, or the times someone can try to break into the network.

#### **►** To specify logon hours

- 1. In the New User dialog box, click Hours.
  - By default, all hours on all days are allowed. This is represented by a filled box for every hour of every day. A filled box indicates that the user is allowed to log on during the hour. An empty box indicates that the user cannot log on.
- Position the mouse pointer on the rectangle on the day and hour that you want to disallow access. Press the mouse button, and drag the pointer through the last hour you want to disallow. The area that you want to disallow should now be shaded.
- 3. Click **Disallow**. The area will still be shaded, but the line indicating hours of access should be gone.
- 4. Repeat steps 2 and 3 for all times that you want the user to be disallowed.
- 5. Click OK.

**Note** A user who is connected to a network resource on the domain is not disconnected when the user's logon hours run out. However, the user will be unable to make any new connections.

## **Setting Workstation and Account Options**



#### **Workstation Access**

Setting workstation access allows you to control which computers a user can use to log on to the domain. This prevents users from accessing another user's local data and can be used to require users to log on to workstations that are in an observed location.

#### ► To specify which workstations a user can access

- 1. In the **New User** dialog box, click **Logon To**. By default, each user account can log on from all computers in the domain.
- 2. Click User May Log On To These Workstations.
- 3. Enter at least one and up to eight computer names that the account can use, and then click **OK**.

#### **Account Information**

The following two options can be set in the **Account Information** dialog box:

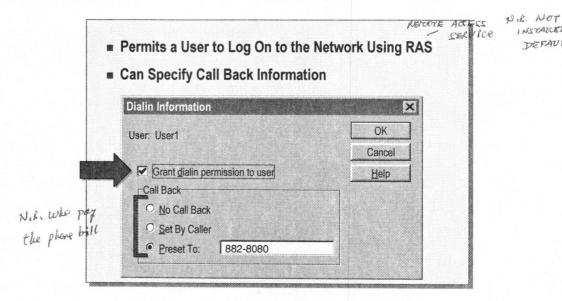
- Account Expires—use this to set a date when the account will be automatically disabled. This is useful for temporary accounts for contractors or part-time employees.
- Account Type—use this to create a local account for a user from an untrusted domain who needs access to a network resource in your domain. A local account can be used to connect to a resource over the network. It cannot be used to log on from a computer in the domain where it was created.

#### **▶** To specify account information

- 1. In the New User dialog box, click Account.
- 2. To specify an expiration date, click End of, and then type a date.
- 3. To specify a local account, click **Local Account**.

INSTALLED BY DEFAULT

## **Granting Dial-in Permission**



Before a user can log on to the network using the Remote Access Service (RAS), they must have dial-in permission assigned to their user account.

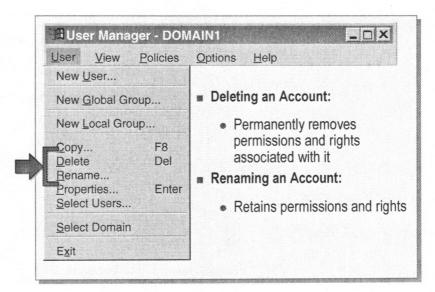
You can also specify that the RAS server will call the dial-in user back; either at a number specified by the user so that the company is billed for the call, or at a number you specify to restrict the user to a specific dial-in location.

### ► To enable dial-in permission

- 1. In the New User dialog box, click Dialin.
- 2. Click the Grant dialin permission to user check box.
- 3. Configure the following call back options.

Option	Description
No Call back	When selected, the RAS server will not call back the user, and the user will incur the telephone charges for the session. This is the default.
Set By Caller	When selected, lets the user specify a telephone number so that the RAS server can call the user back. This means that the organization that owns the RAS server will incur the telephone charges for the session.
Preset To	When selected, lets you specify a telephone number that the RAS server will use to call back the user. This reduces the risk of an unauthorized person using the user's account, because the user must be at the specified phone number in order to connect to the RAS server. In high security networks, use this option and restrict users to dialing in from only one telephone number.

# **Deleting and Renaming User Accounts**



When an account is no longer needed, you can delete an account or rename an account for use by another user. The following table describes the situation in which you should delete or rename an account.

Do this	When
Delete an account	The account is no longer needed. When an account is deleted, all of the account information is lost. This information includes account properties, rights, permissions, and group memberships. The Administrator and Guest accounts cannot be deleted.
Rename an account	You want to retain all rights, permissions, and group memberships for the account for a different user. For example, when a new employee replaces another employee, rename the user account and have the new employee change his or her password when he or she first logs on.

#### ► To delete a user account

- 4. Start User Manager for Domains, and then select the user account.
- 5. Press the DELETE key or, on the  $\boldsymbol{User}$  menu, click  $\boldsymbol{Delete}.$

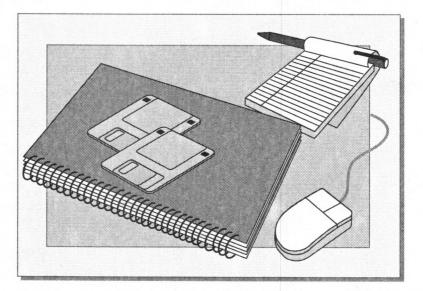
A dialog box appears warning you that once the account is deleted, even recreating it will not make the resources available to the newly created account that were available to the account that you deleted.

6. Click **OK** and the user account is deleted.

#### To rename a user account

- 1. Start User Manager for Domains, and then select the user account.
- 2. On the User menu, click Rename.
- 3. In the Change To box, type in the new user name, and then click OK.

# **Lab 1: Planning and Creating User Accounts**



# Managing the User Work Environment

ie. network connections desktop settings

#### A User Profile

- . Is created by default for each user
- Defines a user's desktop environment
- Retains network and printer connections
- Can be customized to restrict available options

### A Logon Script

- Configures network and printer connections for non-Windows NT-based clients
- Cannot configure the desktop environment

C:/WINT/ Profiles

### **User Profiles**

When a user logs on for the first time from a Windows NT-based client, a default user profile is created for that user. The user profile defines such things as the appearance of a user's desktop environment and the user's network and printer connections. A user profile can also be customized to restrict what users see in their interface and have available to use when they log on. For example, an administrator can remove the Administrative Tools folder to prevent a user from changing a configuration.

User profiles contain all user-definable settings for the work environment of a computer running Windows NT. All user-specific settings are automatically saved in the Profiles folder within the system root folder (C:\Winnt\Profiles).

### **Logon Scripts**

For users who log on from non-Windows NT-based clients (LAN Manager, MS-DOS®, Windows for Workgroups, and Windows 3.x), a logon script can be used to configure users network and printer connections. Logon scripts cannot be used to define the appearance of a user's desktop environment or hardware settings, such as video display resolution.

A logon script is a batch (.bat or .cmd) file or an executable (.exe) file that runs automatically when a user logs on to the network.

**Note** For more information on the settings stored in a user profile, see *Concepts and Planning, Microsoft Windows NT Server*. For more information on logon scripts, see *Concepts and Planning, Microsoft Windows NT Server* and the *Microsoft Windows NT Server Resource Kit*.

UNC path name -> Neonputername | Sharename Universial Noming Convention

### **Roaming User Profiles**

### **■ Roaming Profile**

- Is applied at any computer the user logs on to
- Centralizes administration of profiles

### **■ Roaming Mandatory Profile**

- Assign to one or many users
- Users cannot modify

### **■ Roaming Personal Profile**

- Assign to one user
- User can modify

Hot-desking

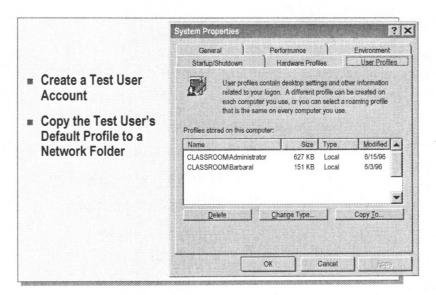
Roaming user profiles provide the user with the same working environment, no matter which Windows NT-based computer the user logs on to. Roaming user profiles are stored centrally on a network server. You can specify a *roaming* user profile for a user account.

You can specify one of the following two roaming profiles:

- Roaming mandatory user profile—this is a preconfigured user profile that the user *cannot* change. One mandatory profile can be assigned to many users. This means that by changing one profile, the administrator can change several desktop environments.
  - You use this type of profile to assign common settings for all users who *require* identical desktop configurations—for example, bank tellers.
- Roaming personal user profile—this is a user profile that a user *can* change; this means that when the user logs off, the user profile is updated to include any changes made by the user. When the same user logs on again, the profile is loaded as it was last saved. If you use roaming personal user profiles, each user should be assigned his or her own profile.

**Note** Windows 95—based clients must be created on a computer running Windows 95, because Windows NT user profiles are not compatible with Windows 95 user profiles. For more information on creating Windows 95 user profiles, see "User Profiles and System Policies," in the *Microsoft Windows 95 Resource Kit*.

### **Creating Roaming User Profiles**



Creating a roaming user profile is a two-step process: creating a test user profile and then copying the test user profile to a network server.

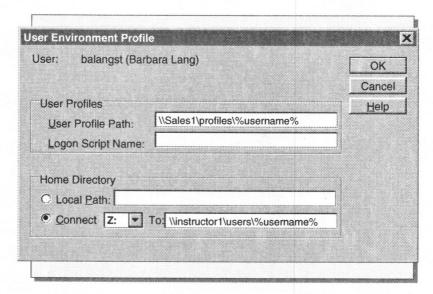
#### ► To create a test user profile

- 1. Create a user account to act as a test user account. For example, create an account named Sales Profile.
- 2. Log on as the test user account. A user profile is automatically created on the local computer in the C:\Winnt\Profiles folder.
- 3. Configure the desktop environment, including appearance, shortcuts, and **Start** menu options.
- 4. Log off, and then log on as Administrator.

#### To copy the test user profile to a network server

- 1. Create a folder on a network drive to store network profiles. For example: \\server\_name\\Profiles\user\_name
- 2. In Control Panel, double-click System, and then click the User Profiles tab.
- 3. Under **Profiles Stored On This Computer**, click the profile that you want to copy, and then click **Copy To**.
- 4. In the Copy Profile To box, type the network path to the folder.
- 5. Under Permitted to Use, click Change.
- 6. Add the appropriate user, and then click **OK**.
- 7. In the folder that you created on the network, rename the file Ntuser.dat to Ntuser.man if this is a mandatory user profile.
- 8. Start User Manager for Domains, double-click the user account, and then, in the **User Properties** dialog box, click **Profile**.
- 9. In the **User Profile Path** box, type the UNC path to the network profile folder. For example: \\server\_name \\Profiles \\user\_name

# **Defining a User's Environment**



You use the **User Environment Profile** dialog box to enter the paths to the user profile, logon script, and home folder.

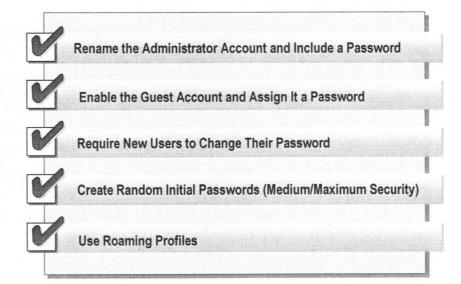
### To specify the locations of user profiles, logon scripts, and home folders

- 1. In the New User (or User Properties) dialog box, click Profile.
- In the User Environment Profile dialog box, configure the following options.

Option	Enter
User Profile Path	The path to the user's profile folder. For personal user profiles, type \\server_name\profile_share\\% username\%
	For mandatory user profiles, type \\server_name\profile_share\profile_name
Logon Script Name	The name of the logon script. You can use a path to the user's local computer or a UNC path to a shared folder on a network server.
Home Directory	The path to the home folder. You can use a path to the user's local computer. For example, \\server_name\\script_share\\script_name.  To specify a network path, select Connect and a drive letter. In the To box, type a UNC (Universal Naming Convention) path (a naming convention for describing network servers). UNC names start with two backslashes followed by the server computer name, and then the shared folder name.  For example: \\server_name\\\users\\\%\\\username\\%\\\username\\\\\\\\username\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

**Best Practice** Use the %Username% variable whenever you create a home folder or personal user profile. This variable will automatically be replaced with the user account name.

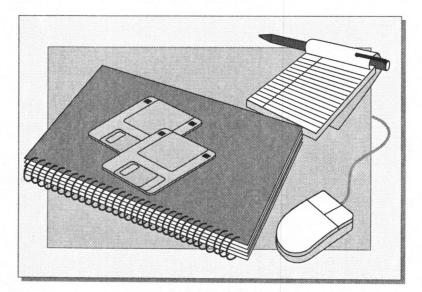
### **Best Practices**



The following list provides best practices for setting up user accounts:

- To provide a greater degree of security, create a user account that you can use to perform non-administrative tasks, rename the Administrator account, and only log on as Administrator to perform administrative tasks.
- Only enable the Guest account in low security networks and always assign it a password. This account is disabled by default.
- Always require new users to change their passwords the first time they log on. This will force users to protect their user account.
- In medium and high security networks, create random initial passwords for all user accounts.
- Use roaming profiles so that each user's working environment will be available when the user logs on from any computer running Windows NT.

# **Lab 2: Configuring User Profiles**



## **Review**

- **Introduction to User Accounts**
- Planning New User Accounts
- **Creating User Accounts**
- Deleting and Renaming User Accounts
- **Managing the User Work Environment**
- **Best Practices**

- 1. Where is the directory database for the domain stored?  $\label{eq:poly} \text{P>C}$
- 2. Where are accounts created in a domain?

master directory laterbese

3. Why would you create home folders on a network server?

EASIER TO BACKUP

4. In a high-security network, what will you want to do to make the Administrator and Guest accounts more secure?

CHG. THE NATIE OF ADMINISTRATOR
USE A TRICKY PASSIVERD
DISABLE GUEST A/C

5. What is the difference between a local and a roaming profile?

LOCAL PROFILE - ON LOCAL MACHINE

ROATING U - ON ONE MACHINE

(in a shared folder in a network server)

# Module 3: Setting Up Group Accounts

# Overview

- **Introduction to Groups**
- Planning a Group Strategy
- Creating Local and Global Groups
- **Implementing Built-in Groups**
- **Best Practices**

### **Objectives**

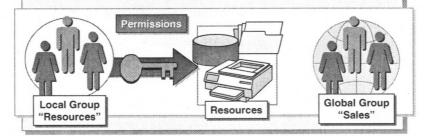
At the end of this module, you will be able to:

- Describe the types of groups available in Microsoft® Windows NT®.
- Compare and contrast local and global group accounts.
- Plan local and global groups.
- Create new local and global groups.
- Delete groups.
- Apply best practices for creating groups.

**Note** This module focuses on how groups are used to simplify administration of user accounts. Application of groups is covered throughout the course.

# **◆** Introduction to Groups

- **Groups Are Collections of User Accounts**
- **Group Members Get All Group Permissions and Rights**
- Local Groups Provide Access to Resources and Rights to Perform System Tasks
- **Global Groups Organize Users**



A group is a collection of user accounts. Assigning a user account membership in a group gives that user all the rights and permissions granted to the group.

Groups simplify administration by providing an easy way to grant common capabilities to multiple users at one time. For example, if several users need to read a file, the user accounts are added to a group. The capability to read is assigned just once, to the group, rather than to each user.

There are two types of groups—local and global:

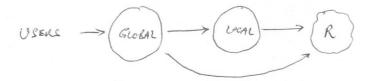
 Local groups are used to provide users with permission to access a network resource.

Permissions are rules that regulate which users can use a resource such as a folder, file, or printer.

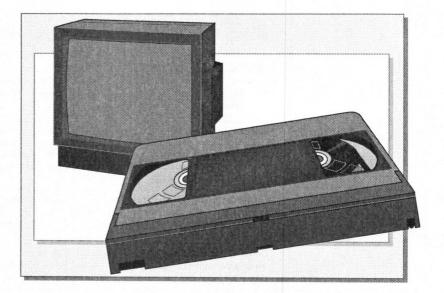
Local groups are also used to provide users with rights to perform system tasks, such as changing the time on a computer or backing up and restoring files. Windows NT includes several pre-created local groups designed specifically to assign users rights. This type of local group is called a *built-in* local group.

• Global groups are used to organize domain user accounts, typically by function or geographical location.

They are typically used in multiple-domain networks, when users from one domain need to access resources in another domain.



# Video: Local and Global Groups



This video defines local and global groups and explains how they are used in single- and multiple-domain networks.

As you view the video, look for the following information:

- What is the purpose of a local group? Global group?
- Where are local groups created? Global groups?

local machine only on PDC.

# **Local and Global Groups Summary**

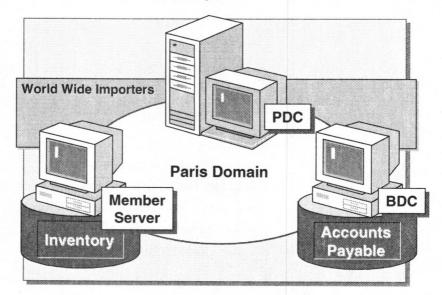
Local Groups	Global Groups	
Provide users with permissions or rights	Organize domain users	
Can include (from any domain): User accounts Global groups	Can only include user accounts in the domain where it resides	
Cannot include other local groups	Cannot contain local or global groups	
Are assigned permissions and rights in the local domain	Are added to a local group to give its members rights	
On a computer running Windows NT Workstation or a member server, can only be assigned to local resources	Are not assigned to local resources  CAN BE! BUT NOT USUALLY!!	
On a PDC, can be assigned resources on any domain controller in the domain	Must be created on a PDC in the domain where the accounts reside	

Both local and global groups must reside in the directory database of the local computer. The following table summarizes the differences between local and global groups.

Local groups	Global groups	
Are used to provide users with permission to access a network resource or rights to perform a system task.	Are used to organize domain user accounts, typically by function or geographical location.	
Can include user accounts and global groups from any domain (with the appropriate trust relationship).  Cannot include other local groups.	Can only include user accounts from its own domain.  Cannot contain local groups or other global groups.	
Are assigned permissions for a resource or granted rights in the local domain.	Are added to a local group in any domain (with the appropriate trust relationship) to give its members access to a resource or grant members rights.	
If created on a member server or computer running Windows NT Workstation, can only be assigned to resources or granted rights on the local computer.	Are not assigned to local resources.	
If created on a PDC, can be assigned to resources or granted rights on any domain controller within the domain.	Are always created on the PDC in the domain where the account resides.	

running User Manager for Domains.

## **Example of Using Local and Global Groups**



#### **Class Discussion**

The Paris office of World Wide Importers has a single-domain network with a PDC, a BDC, and a member server. The BDC has an accounts payable database, and the member server has an inventory database. All users need access to both databases.

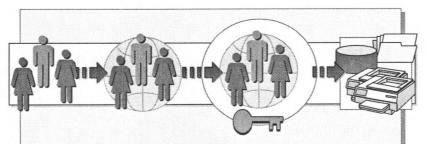
1. On which computer would you create a global group for organizing the user accounts? Why?

2. On which computer would you create a local group to provide users with access to the Accounts Payable database? Why?

3. On which computer would you create a local group to provide users with access to the Inventory database? Why?

MEMBER SERVER

# **Planning a Group Strategy**



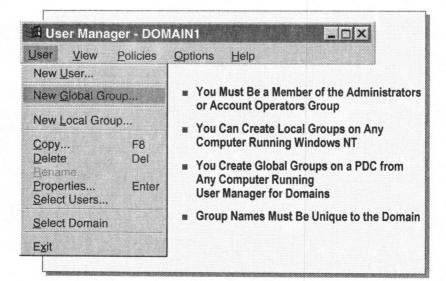
- **Logically Organize Users Based on Common Needs**
- Create Global Groups, and then Add User Accounts
- Create Local Groups Based on Resource Access Needs
- Assign Permissions to Local Groups
- Add Global Groups to Local Groups

When creating groups, follow these guidelines:

- Organize domain users logically based on common needs. For example, if all sales personnel need access to a color printer and all managers need access to an employee records file, organize users by sales personnel and managers.
- In each domain where user accounts reside, create a global group for each logical group of users. Then add the appropriate user accounts to the appropriate global groups.
- Create local groups based on resource access needs. For example, if managers need full control of files in the \EmployeeHandbook directory and sales personnel only need to read the files, create one local group for the managers and another local group for the sales personnel.
  - If the resource is on a member server or a computer running Windows NT Workstation, create the local group where the resource is located.
  - If the resource is on a primary domain controller (PDC) or backup domain controller (BDC), create the local group on the PDC.
- Assign the appropriate permissions to the local groups.
- Add the global groups to the local groups.

**Note** To add global groups from one domain to local groups in another domain, the appropriate trust relationship must have been established.

# Creating Local and Global Groups



CAL ADMINISTRATOR

GLOUP - MOST
POWERFUL

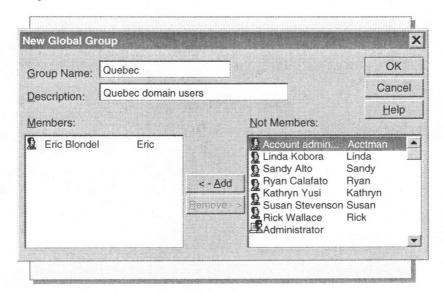
On Windows NT Server, local and global groups are created using User Manager for Domains.

On Windows NT Workstation, local groups are created using User Manager. Global groups cannot be created.

When you create local and global groups, the following rules apply:

- You must be a member of the Administrators or Account Operators group.
- A local group can be created on any computer running Windows NT.
- A global group must be created on a PDC, but can be created from any computer running User Manager for Domains. This includes:
  - A BDC.
  - A member server that is part of the domain.
  - A computer running Windows NT Workstation or Microsoft Windows® 95 with the Windows NT Server Administrative Tools installed.
- Group names must be unique to the domain. They cannot be identical to other user names or group names.

### **Creating Global Groups**



The first part of your implementation strategy should always be to logically organize your users and to create global group accounts for them.

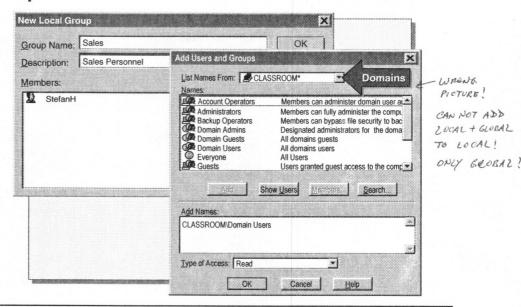
#### ► To create a global group

- 1. On the User menu, click New Global Group. The New Global Group dialog box appears.
- 2. In the **Group Name** box, type the name of the group. The global group name:
  - Can contain any uppercase or lowercase characters except for the following: "/\[]:; |=,+?<>.
  - Should describe the function of the group.
  - Is limited to 20 characters.
- 3. In the **Description** box, type a description of the group. Although the description is optional, it can be helpful in identifying the function of a group.
- 4. In the **Not Members** list, select the users you want in the group.

**Tip** As a shortcut to adding users to a global group, press the CTRL key, select each user you want to add to the group, and then on the **User** menu, click **New Global Group**.

- 5. Click **Add**. The users you selected appear in the **Members** list.
- 6. Click **OK** to create the global group containing all the users you added as members.

### **Creating Local Groups**



#### ► To create a local group

- 1. On the **User** menu, click **New Local Group**. The **New Local Group** dialog box appears.
- 2. In the **Group Name** box, type a unique, descriptive name for the group. The name:
  - Should describe the function of the group.
  - Can contain any uppercase or lowercase characters except for the backslash character (\).
  - Can be up to 256 characters in length; however, only the first 22 characters display in most of the windows.
- 3. In the **Description** box, type a description of the group, and then click **Add**. The **Add Users and Groups** dialog box appears.
- 4. In the **Names** list, select the user or global group accounts from the local domain you want added to the group.

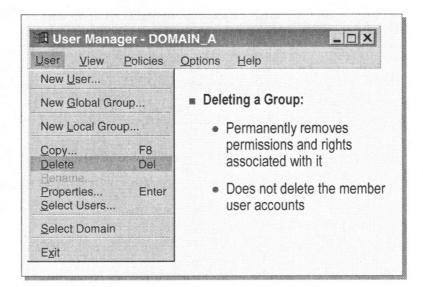
**Tip** As a shortcut to adding users and global groups from the local domain to a local group, press the CTRL key, select each user you want to add to the group, and then on the **User** menu, click **New Local Group**.

5. To add global groups from another domain, in the **List Names From** box, select the domain, and then select the global groups. The asterisk indicates the current domain.

**Note** The **List Names From** box shows only the trusted domains. If a domain name does not appear in this box, the appropriate trust relationship is not set up.

- 6. Click Add, and then click OK.
- 7. Click **OK** in the **New Local Group** dialog box to create the local group.

### **Deleting Groups**



Deleting a group deletes the name of the group, its description, and the rights or permissions associated with it. It does not delete the user accounts it contains.

#### ► To delete a group account

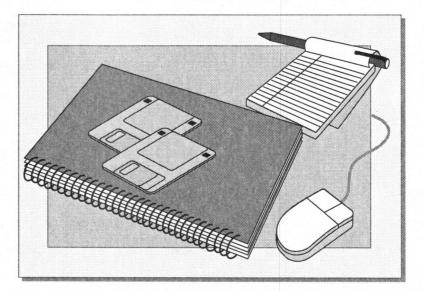
- 1. Start User Manager or User Manager for Domains.
- 2. Select the group you want to delete.
- 3. Press the DELETE key.

The following message appears:

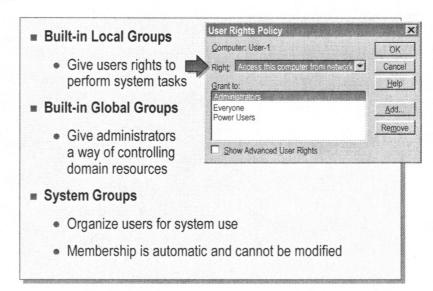
Each group is represented by a unique identifier which is independent of the group name. Once this group is deleted, even creating an identically named group in the future will not restore access to resources which currently name this group in the access control list.

4. Click **OK**.

# Lab 3: Planning and Creating Local and Global Groups



# Implementing Built-in Groups



Built-in groups are predefined groups that have a predetermined set of user rights. User rights determine the system tasks a user or member of a built-in group can perform.

Computers running Windows NT have three types of built-in groups:

 Built-in local groups give users rights to perform system tasks such as backing up and restoring files, change the system time, and administering system resources.

Built-in local groups are on all computers running Windows NT.

■ Built-in global groups give administrators an easy way of controlling all users in a domain.

Built-in global groups are on domain controllers only.

• System groups automatically organize users for system use. Administrators do not assign users to them. Rather, users are either members by default or become members during network activity.

System groups are on all computers running Windows NT.

**Note** Built-in groups cannot be deleted or renamed.

- Back up the security database

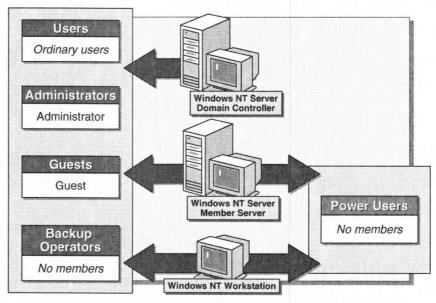
- use Energency Recovery Dick (N.B. it contains the Administrator, Guest (Disabled) 4

other users abready created @ the time the disk is created)

- erecte a user (ie. fred) I put him in the Administrator group.

put his nome/passworld in a safe for emergency purpose.

# **Built-in Groups on All Windows NT-Based Computers**



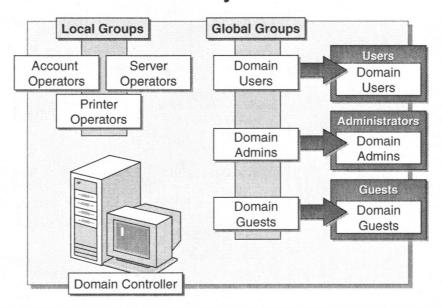
All computers running Windows NT have built-in groups. A built-in group on a domain controller determines what its members can do on the domain. A built-in group on non-domain controllers determines what its members can do on the local computer.

The following table describes the built-in local groups that reside on all computers running Windows NT.

Local group	Capabilities
Users	Perform tasks for which they have been granted rights and access resources to which they have been assigned permissions.
Administrators	Can perform all administrative tasks on the local computer. If the computer is a domain controller, members can fully administer the domain.
Guests	Perform tasks for which they have been given rights and access resources to which they have been assigned permissions.
	Members of Guests cannot make permanent changes to their local environment.
Backup Operators	Use the Windows NT Backup program to back up and restore all computers running Windows NT.
Replicator	Used by the Directory Replicator service. This group is not used for administration.

**Note** The local Power Users group only resides on member servers and computers running Windows NT Workstation. Power Users group members can create and modify accounts, and they can share resources.

## **Built-in Groups on Domain Controllers Only**



### **Local Groups**

The following table describes the built-in local groups on domain controllers only. There are no initial members of these groups.

Local Group	Capabilities
Account Operators	Create, delete, and modify users, global groups, and local groups. Cannot modify the Administrators or Server Operators groups.
Server Operators	Share disk resources, and back up and restore the server.
Printer Operators	Set up and manage network printers.

#### **Global Groups**

When Windows NT Server is installed as a domain controller, three global groups are created in the domain's directory database—Domain Admins, Domain Users, and Domain Guests. By default, built-in global groups do not have any inherent rights. They get rights when they are added to local groups or when they are assigned user rights or permissions.

The following table describes what happens to built-in global groups when a Windows NT-based computer is added to the domain.

This group	Is automatically added to the
Domain Users	Local Users group. When a domain user account is created it is automatically made a member of this group. The Administrator account is a member by default.
Domain Admins	Local Administrators group. Members of the Domain Admins group can then perform administrative tasks on the local computer. The Administrator account is a member by default.
Domain Guests	Local Guests group. The Guest account is a member by default.

## **Built-in System Groups**

- **Reside on All Computers**
- **Membership Cannot Be Modified**
- Users Become Members Automatically During Network Activity
- **Two Key System Groups** 
  - Everyone
  - Creator Owner

Built-in system groups reside on all computers running Windows NT. Users become members by default during network activity. Membership cannot be modified.

The following table describes the key system groups used for network administration.

System group	Description
Everyone	Includes all local and remote users who access the computer. Unlike the Domain Users group, the Everyone group contains user accounts other than those created by the administrator in the domain. Administrators can assign permissions and rights to the group Everyone.
Creator Owner	Includes the user that created or took ownership of a resource. If a member of the Administrators group takes ownership of a resource, it is proper the new owner is the Administrators group. This group can be used to manage access to files and folders only on NTFS volumes.

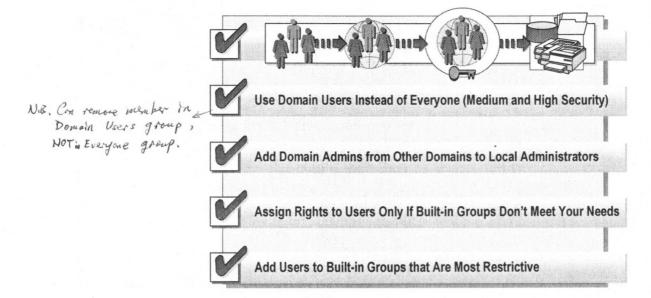
The following table describes the system groups that are not used for network administration.

System group	Description
Network	Includes any user who is currently connected from another computer on the network to a shared resource on your computer.
Interactive	Automatically includes a user who logs on to the computer locally. Interactive members access resources on the computer at which they are physically sitting. They log on and access resources by "interacting" with the computer.

**Note** The Everyone and Creator Owner groups are covered in more detail later in the course.

N.B. The user who print something automatically become anember of the Crenter Owner group.

### **Best Practices**

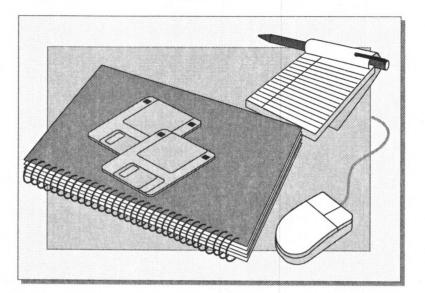


The following list provides the best practices for implementing local and global groups:

- Apply the following strategy when using local and global groups:
  - Organize users into global groups
  - Assign permissions to local groups
  - · Add global groups to local groups
- Use the global group Domain Users instead of the Everyone group. The Domain Users group contains only accounts you've created, and not all accounts that have connected to the network.
- To enable the Administrators group to perform administration tasks in other domains, add the global group Domain Admins to the local Administrators group on the computer in the domain you want Administrators to administer.
- If the rights of a built-in group meet your needs, add a user account to the group. Otherwise, create a local group, and then assign the appropriate user rights.
  - For example, if for security reasons you want a user to have the right to back up files but not restore files, create a local group *Backup Only* and assign it the Backup Files and Directories user right.
- Always add users to built-in groups that are most restrictive, while still allowing them to accomplish any tasks.

Reservee (> access control list

# Lab 4: Implementing Built-in Groups



# **Review**

- **Introduction to Groups**
- Planning a Group Strategy
- Creating Local and Global Groups
- **Implementing Built-in Groups**
- **Best Practices**

1. What is the purpose of a local group? Global group?

for allocating monaging user a/e

- 2. What is the difference between a built-in local group and a built-in global group?

  has to to of permission has no
- 3. What enables an administrator to perform administrative tasks on any computer in the domain?

add Domain Admine into local Administrator group

4. What is the recommended strategy for implementing local and global groups?

global k give access to resources.

5. What is the difference between the Domain Users group and the Everyone group?

Can delete member from Domain Users but not from Everyone group.

# Module 4: Administering User and Group Accounts

# Overview

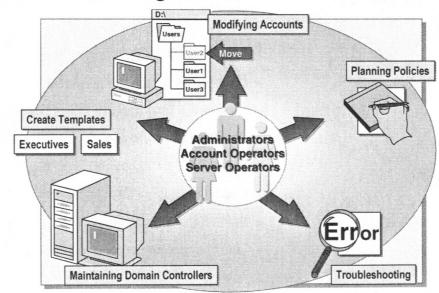
- **Introduction to Administering Accounts**
- Creating User Account Templates
- Implementing an Account Policy
- Resetting User Account Passwords
- **Unlocking User Accounts**
- **Modifying Multiple User Accounts**
- Maintaining Domain Controllers
- **Troubleshooting Logon Problems**

#### **Objectives**

At the end of this module, you will be able to:

- Create a template and use it to create user accounts.
- Implement an account policy for all accounts in a domain.
- Reset user account passwords.
- Unlock a user account.
- Change the location of a home directory.
- Promote a backup domain controller (BDC) to a primary domain controller (PDC).
- Restore a primary domain controller.
- Synchronize domain controllers.
- Troubleshoot logon problems.

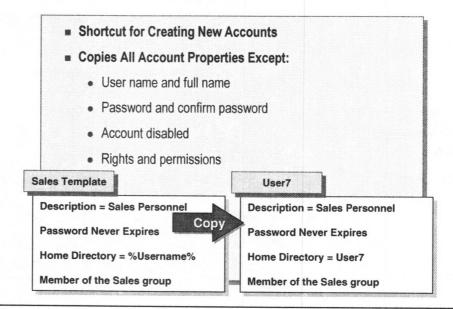
# **Introduction to Administering Accounts**



There are procedures and tools an administrator can use to perform daily tasks efficiently and to keep the network running smoothly. Some of these are:

- Creating templates for adding new user accounts.
- Making changes to multiple user accounts at one time, such as moving home folders.
- Planning and implementing an account policy to keep the network secure.
- Maintaining domain controllers so that user accounts can always be successfully validated.
- Troubleshooting any problems users have with their accounts; these are primarily problems users have logging on.
- Distributing some of the administrative tasks by creating an additional Administrator or an Account Operator.
  - Members of the Administrators group have full administrative capabilities. They are responsible for planning and maintaining network security.
  - Members of the Account Operators group can create, delete, and modify user accounts, global groups, and local groups, and set account policies.

# Creating User Account Templates



A user account template is a standard user account that you create with the properties that apply to users with common needs. For example, if all sales personnel require membership in the Sales group, you can create a template that includes membership to that group.

To use a template to create a new user account, you just copy the template account and assign a user name and password for the new user. The following options become properties of the new user account:

Description	Profile	
User Must Change Password at Next Logon	Hours (domain controllers only)	
<b>User Cannot Change Password</b>	Logon to (domain controllers only)	
Password Never Expires	Account (domain controllers only)	
Groups	Dialin	

**Note** Rights and permissions granted to an individual user account are not copied.

Some suggestions for creating templates are:

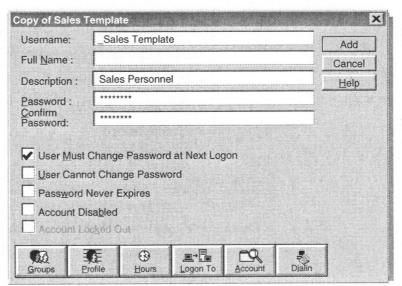
- Make a template for each classification of employee, such as sales, accountants, managers, and so on.
- If you commonly have short-term or temporary network users, create a template with limited logon hours, workstation specifications, and other necessary restrictions.

**Tip** If you begin each template name with a non-alphabetic character, such as the underscore character (\_), the template will always appear at the top of the list the User Manager window.

# **Using Templates to Create User Accounts**

N.B. Password is used here to prevent user logon as the template.

Better Disable the Account !!



To use a template account to create a new user account, copy the template.

#### ► To copy a template account

- 1. Start User Manager or User Manager for Domains.
- 2. In the Username list, select the template you want to copy.
- 3. On the User menu, click Copy.
- 4. Type a user name and password for the new account, and then click Add.
- 5. Create another new user or click Close.

# Implementing an Account Policy

- The Account Policy Determines How Passwords Must Be Used by All User Accounts
- **The Account Policy Sets the Requirements for:** 
  - · Password age, length, and uniqueness
  - Account lockout
- Policy Changes Go Into Effect Either:
  - The next time a user logs on
  - The next time a user makes a change covered by the policy

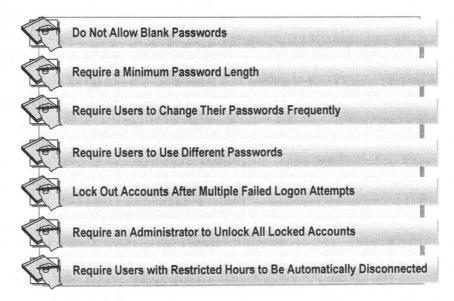
The account policy determines how passwords must be used by all user accounts. It sets the requirements for:

- Password minimum and maximum ages
- Password minimum length
- Password uniqueness
- Account lockout options

Changes you make to the account policy go into effect for users at one of two times:

- The next time the user logs on.
- The next time the user makes a change covered by the policy—for example, the minimum password length does not apply to existing passwords, but it will apply the next time a user changes his or her password.

## **Planning an Account Policy**

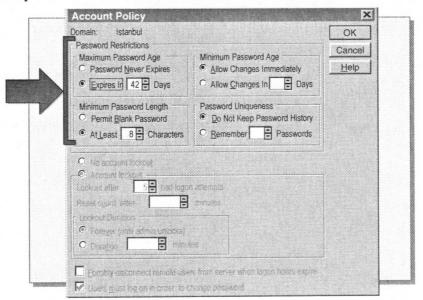


By default, the only password requirement for user accounts is that users change their passwords the first time they log on. To use an account policy to provide additional security for user accounts, consider the following:

- Never allow blank passwords. Blank passwords mean no security. They should never be used on any system connected to the Internet or with dial-in capabilities.
- Require a minimum length for all passwords. The longer the password, the more difficult it is to guess.
  - In a medium-security network, require 6–8 characters.
  - In a high-security network, require 8–14 characters.
- Require users to change their passwords frequently. This helps prevent unauthorized users from guessing it.
  - In a medium-security network, change passwords every 45–90 days.
  - In a high-security network, change passwords every 14-45 days.
- Require users to use a different password each time they change it. Make sure that once it is changed, it cannot be changed back to a previous password.
  - In a medium-security network, require 8–12 different passwords.
  - In a high-security network, require 12–24 different passwords.

- Lock out accounts after multiple failed logon attempts. This reduces the chance of an unauthorized person gaining access to the network.
  - In a medium-security network, lock out a user account after 5 failed logon attempts.
  - In a high-security network, lock out a user account after 3 failed logon attempts.
- Require the administrator to unlock all locked accounts.
- Require that users with restricted logon hours are disconnected from the network during off hours. This will prevent users from dialing in to the network..

# **Setting Password Options**



Account policies allow control over how passwords are implemented.

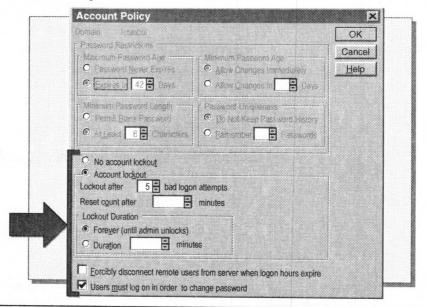
#### ► To set an account policy

- 1. Start User Manager for Domains.
- 2. On the Policies menu, click Account.
- 3. Set the password options as described in the following table.

Option	Description
Maximum Password Age	The period of time a password can be used before the user is required to change it.
	Range of values: 1-999 days.
Minimum Password Age	The period of time a password must be kept before the user can change it. Do not allow immediate changes if a password uniqueness value will be entered. The <b>Minimum Password Age</b> must be less than the <b>Maximum Password Age</b> .
	Range of values: 1–999 days.
Minimum	The minimum number of characters required in a password.
Password Ran	Range of values: 1–14 characters.
Password Uniqueness	The number of new passwords that must be used by a user before an old password can be reused. For uniqueness to be effective, immediate changes should not be allowed by the <b>Minimum Password Age</b> parameter.
	Range of values: 1–24 passwords.

**Important** The **Password Never Expires** check box for an individual user account overrides the **Maximum Password Age** setting.

# **Setting Account Lockout Options**



1. Set an account lockout policy described in the following table.

	Option	Description	
	No account lockout	User accounts are never locked out, no matter how many incorrect logon attempts are made using the account.	
	Account lockout	If you select <b>Account lockout</b> , the next three options are available.	
	Lockout after	The number of incorrect logon attempts that will cause the account to be locked.	
		Range of values: 1–999.	
	Reset count after	The maximum number of minutes that can elapse between any two bad logon attempts before lockout occurs.	
		Range of values: 1–99999 minutes.	
	Lockout Duration	<b>Forever</b> : Causes locked accounts to remain locked until an administrator unlocks them. (The administrator account set up during installation cannot be locked out.)	
		<b>Duration</b> : Causes accounts to remain locked for the specified number of minutes.	
		Range of values: 1–99999 minutes.	
	Forcibly disconnect	If selected, the user account is disconnected from any server in the domain when the account exceeds logon hours.	
the Domain Controller ie. the server	remote users" from server	If cleared, the user account is not automatically disconnected, but no new connections are allowed.	
	when logon hours expire	(Available only on Microsoft® Windows NT® Server.)	
	Users must	If selected, users cannot change (their own) expired passwords.	
	log on in order to change password	If cleared, users can change their own expired passwords.	
		they can chg. their posswords during logar.	

2. Click **OK** to set the policy.

# **Resetting User Account Passwords**

- **Reset Passwords When** 
  - They expire
  - Users forget them
- From User Manager for Domains, Double-Click the Account
  - Delete the password
  - Enter a new password

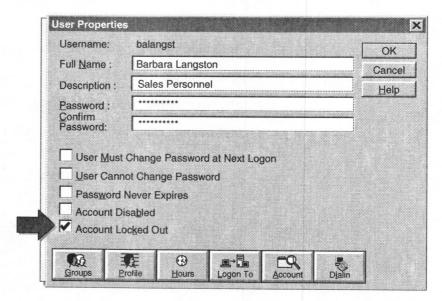
You may need to reset a user's password if:

- The password expires.
- A user forgets his or her password.

#### ► To reset a password

- 1. Start User Manager or User Manager for Domains.
- 2. Double-click the user account.
- 3. In the Password box, select the entire entry, and then press DELETE.
- 4. In the **Confirm Password** box, select the entire entry, and then press DELETE.
- 5. In the **Password** and **Confirm Password** boxes, enter a new password for the user, and then click **OK**.

# **Unlocking User Accounts**



If you have an account policy set up that locks out the user after several failed logon attempts, you may need to unlock the account.

#### ► To unlock a user account

- 1. Start User Manager for Domains.
- 2. In the **Username** list, double-click the user account that needs to be unlocked.

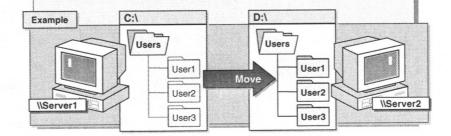
The User Properties dialog box appears.

- 3. Click to clear the Account Locked Out check box.
- 4. Click OK.

**Tip** If the user has failed several times in trying to log on to the domain, the user may have forgotten the password. In this case, you should reset the password while you are unlocking it.

# **Modifying Multiple User Accounts**

- **Shortcut for Modifying Multiple User Accounts**
- **Select Multiple Users**
- Select Properties You Want to Modify
- Enter Change Once to Affect All Selected Users



Use this procedure when you need to modify multiple user accounts in the same manner. For example, you need to move home directories to another server or volume, or set the logon hours for 100 users.

#### ► To modify multiple user accounts at one time

- 1. Start User Manager or User Manager for Domains.
- 2. Select all the user accounts that you want to modify by using one of the following methods.

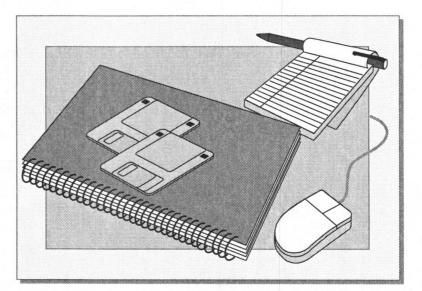
To select accounts in random order, click the first account, press the CTRL key, and then click the remaining accounts.

-or-

To select accounts in consecutive order, click the first account, press the SHIFT key, and then click the last account.

- 3. On the User menu, click Properties.
  - The User Properties dialog box appears.
- 4. Make the necessary changes.
- 5. Click OK.

# **Lab 5: Managing Accounts**



# Maintaining Domain Controllers

#### ■ When You Need to Take a PDC Offline

- Promote a BDC to a PDC to take its place
- When the PDC is back online, promote it back to a PDC

#### ■ When a PDC Goes Offline Unexpectedly

- Promote a BDC to a PDC to take its place
- When the PDC is back online, demote it to a BDC
- Promote it back to a PDC

Maintaining domain controllers means making sure that a primary domain controller (PDC) is always online and that all copies of the directory database are current.

Every domain has only one PDC. The PDC maintains the master copy of the domain's directory database. The directory database is automatically replicated to all the backup domain controllers (BDCs) in the domain every five minutes.

If the PDC goes offline for any reason, users will still be able to log on and be validated by the BDC. But you will no longer be able to do any account administration.

#### When a PDC Needs to Be Taken Offline

When a PDC needs to be taken offline, you need to perform the following steps:

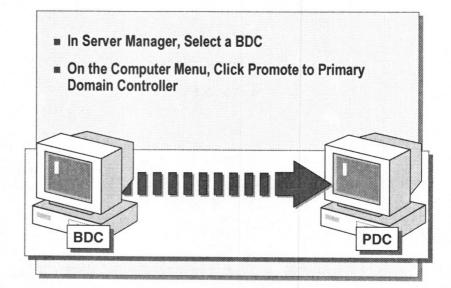
- 1. Promote a BDC to take the place of the PDC while its offline. This will force the PDC to become a BDC.
- 2. When the original PDC is brought back online, promote it back to a PDC, which forces the temporary PDC to demote itself to a BDC.

## When a PDC Goes Offline Unexpectedly

When a PDC goes offline unexpectedly, you need to perform the following steps:

- 1. Promote a BDC to take the place of the PDC.
- 2. Once the original PDC is fixed and brought back online, demote it to a BDC. This will force the temporary PDC to become a BDC.
- 3. Promote the original PDC again.

# **Promoting a Backup Domain Controller**



When you promote a BDC, an up-to-date copy of the domain directory database is replicated from the old PDC to the new one. The original PDC is automatically demoted to a BDC.

#### ► To promote a BDC to a PDC

- 1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Server Manager**.
- 2. In the **Computer** list, select the backup domain controller.
- 3. On the Computer menu, click Promote to Primary Domain Controller.

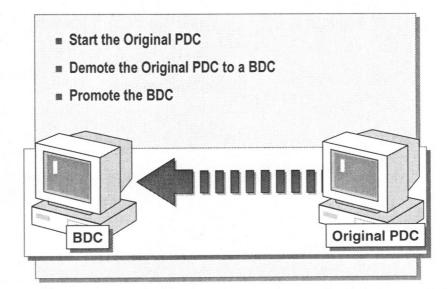
  You receive a message that informs you that the promotion will take a few

You receive a message that informs you that the promotion will take a few minutes, and that all user connections to the BDC and PDC will be closed. It asks you to confirm the change.

4. Click Yes.

When you complete this procedure, the original PDC automatically becomes a BDC.

## **Resuming Domain Controller Roles**



You can also promote a BDC to a PDC after the PDC has gone offline, but the PDC will not automatically be demoted. Also, since the PDC is offline, no automatic replication of the accounts database can occur between the two PDCs.

When the original PDC is brought back online, there is already a PDC in the domain, so its Net Logon service will fail to start. You will need to restore the original PDC.

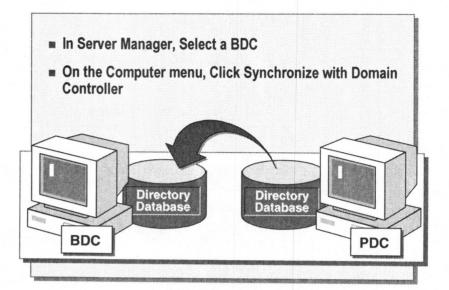
#### ► To return the original PDC to the role of PDC

- 1. Start the computer that was originally functioning as the PDC. As it starts up, it will detect that there is already a PDC in the domain.
- Start Server Manager on the original PDC.
   Both the original and current PDC appear as primary domain controllers, but that the original PDC name is unavailable.
- 3. Select your original PDC.
- 4. On the Computer menu, click Demote to Backup Domain Controller.
- 5. Select the BDC that was the original PDC, and on the **Computer** menu, click **Promote to Primary Domain Controller**.
- 6. Click Yes to make the change.

You will receive messages indicating that the directory database on the current PDC was synchronized with the directory database on the current BDC before it is promoted to a PDC.

If any administration, such as adding user accounts or changing passwords, was done while the original PDC was down, this automatic synchronization of the directory databases ensures that these changes are not lost.

# **Synchronizing Domain Controllers**



You can manually synchronize domain controllers:

- To apply changes made to the domain's directory database immediately.
- To solve problems related to password mismatches. If users change their passwords, it takes time for new passwords to be distributed automatically to all the BDCs in a large domain.

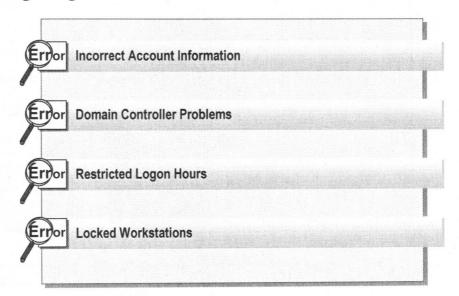
#### ► To synchronize a specific BDC

- 1. Start Server Manager, and then select the BDC.
- 2. On the Computer menu, click Synchronize with Primary Domain Controller. You receive a message that informs you that the process may take a few minutes, and it asks you to confirm the change.
- 3. Click **Yes**. A message appears telling you that the selected BDC will synchronize its account database with the PDC. It tells you to check the event log on the selected BDC and on the PDC to determine whether the synchronization was successful.
- 4. Click OK.

#### ► To synchronize all domain controllers

- 1. Start Server Manager, and then select the PDC.
- 2. On the **Computer** menu, click **Synchronize Entire Domain**. A message informs you that the process may take a few minutes, and it asks you to confirm the change.
- 3. Click **Yes**. A message box informs you that the PDC has asked all BDCs to start synchronizing their user account database, and it suggests that you check the Event Log to determine whether synchronization was successful.
- 4. Click OK.

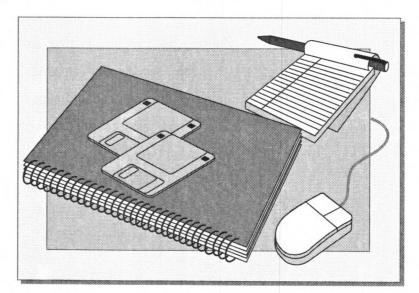
# **Troubleshooting Logon Problems**



The following table describes common error messages and solutions to logon problems.

User error message	Solution	
The system could not log you on. Make sure your user name and domain name are correct, and then type your	Verify that the user name, domain name, and password are correct; check the CAPS LOCK key—passwords are case sensitive. (The domain name can be verified using the Control Panel Networks application.)	
password again. Letters in passwords must be typed using the correct case. Make sure that CAPS LOCK is not accidentally on.	If a user has forgotten the password, delete or reset the user's password.	
	If the user account is new, it may not have been synchronized with BDCs. Synchronize domain controllers.	
A domain controller for your domain could not be	Check to see if this is the only computer having difficulty. Verify that the domain controllers are online.	
contacted. You have been logged on using cached account information. Changes made to your profile since you last logged on may not be available.	If the PDC is still online, select a BDC and promote it to a PDC. If the PDC is offline, promote a BDC to a PDC.	
	If it is the only computer having the problem, verify that the cable connects the computer to the network. Verify that the network adapter card light is on or is blinking. If the problem is not obvious, restart the computer.	
Your account has time restrictions that prevent you from logging on at this time. Please try again later.	The logon hours for the user are not allowed for the current time. To allow a user to log on, modify the user's logon hours.	
Your account is configured to prevent you from using this workstation. Please try another workstation.	The user has been restricted from using that workstation. To allow the user to use the workstation, modify the <b>Logon To</b> restrictions.	

# **Lab 6: Managing Domain Controllers**



# **Review**

- Introduction to Administering Accounts
- **Creating User Account Templates**
- **Implementing an Account Policy**
- **Resetting User Account Passwords**
- Unlocking User Accounts
- **Modifying Multiple User Accounts**
- Maintaining Domain Controllers
- Troubleshooting Logon Problems
- 1. When and why would you create a template for creating new user accounts? When a number of users have similar requirements.
- 2. What is included in the account policy and why is it important?

  IT DEFERATINE HOW SECURE THE NETWORK IS.
- 3. If your PDC has gone offline unexpectedly, what do you need to do to maintain the directory database?

PROMOTE BAC

4. What are some possible reasons why a user cannot log on?

Module 5: Securing Network Resources with Shared Folder Permissions

# Overview

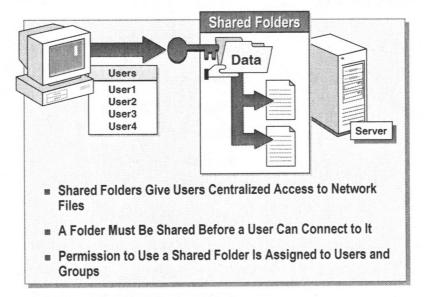
- Introduction to Shared Folders
- **Guidelines for Sharing Folders**
- Sharing Folders
- Accessing Shared Folders
- **Best Practices**

## **Objectives**

At the end of this module, you will be able to:

- Describe the shared folder permissions.
- Describe the result when user and group permissions are combined.
- Plan what permissions to assign to groups or users for network applications, data, and home folders.
- Create and modify shared folders in single-domain and multiple-domain networks.
- Assign shared folder permissions to users and groups in single-domain and multiple-domain networks.
- Connect to shared folders.
- Apply the best practices for administering shared folders.

# ◆ Introduction to Shared Folders



When accessing reseource which two group a user belong to have access, the access right of the less restrictive group will be used!

Except the NO ACCESS will overwritten all right!

## What Is Sharing?

Sharing is a feature of Microsoft® Windows NT® that enables you to designate resources that you want users to access across the network. When a folder is shared, users can connect to the folder over the network and access the files that it contains.

You assign *shared folder permissions* to control what users can do with the contents of a shared folder. For example, if a user needs only to view files in a shared folder, you can assign Read permission; if a user needs to add or remove files, you can assign Change permission. A shared folder appears in Windows NT Explorer and My Computer as an icon of a hand holding the shared folder.

**Important** Once a *folder* is shared, users with the appropriate permissions have access to all files and folders within the shared folder.

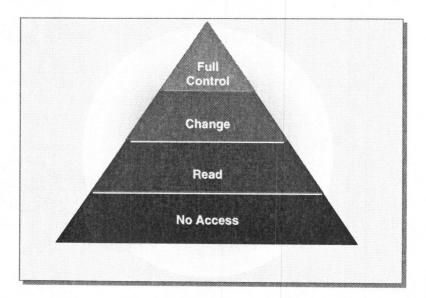
## Why Share Folders?

Shared folders are used to give users access to network applications, data, and user home folders:

- Network application folders centralize administration by designating one location for configuring and upgrading software. In this way, you avoid maintaining applications on clients.
- Data folders provide a central location for users to store and access common files
- User home folders provide a central location for backing up users' data.

**Note** Using shared folders is the only way to secure network resources on a FAT volume.

## **Shared Folder Permissions**

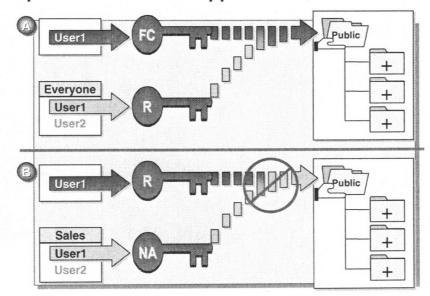


To control how users access a shared folder, you assign *shared folder permissions*. Permissions can be assigned to users, groups, or both. The following table describes the shared folder permissions, from most restrictive to least restrictive.

This permission	Lets users	
Full Control (default)	Change file permissions.  Take ownership of files on NTFS volumes.  Perform all tasks permitted by the Change permission.  (The default permission assigned to the Everyone group.)	
Change	Create folders and add files. Change data in, and append data to, files. Change file attributes. Delete folders and files. Perform all tasks permitted by the Read permission.	
Read	Display folder names and file names.  Display the data and attributes of files.  Run program files.  Change to folders within a folder.	
No Access	Establish only a connection to the shared folder. Access to the folder is denied and the contents do not appear.	

**Important** Shared folder permissions are effective only when a user connects to the folder over the network. Users with the user right "Log on locally" can sit at the computer and access the computer's hard disk directly, bypassing shared folder permissions. However, the user may be restricted by local NTFS permissions.

# **How User and Group Permissions Are Applied**



A user can be assigned permissions to access a shared folder directly or as a member of a group. Also, a user may be a member of multiple groups with different permissions that provide different levels of access.

Permissions are applied in the following ways:

A When a user is assigned permission to a shared folder, and that user is a member of a group to which a different permission is assigned, the user's effective permissions are the combination of the user and group permissions.

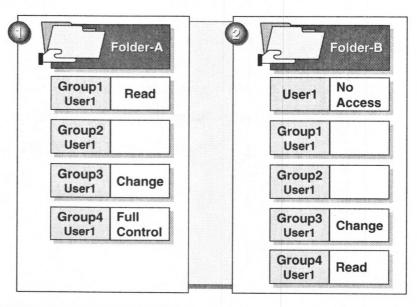
For example, if a user has been assigned Read permission for the Public folder, and the Everyone group has been assigned Full Control permission to the same folder, the permissions combine, so that the effective permission is Full Control.

B The only exception to this rule is the No Access permission. The No Access permission always overrides any other permissions assigned to a user or to any group to which the user belongs.

For example, if a user has been assigned the Read permission for the Public folder, and the user is a member of the Sales group that has been assigned No Access to the same folder, then the user's effective permission is No Access.

**Note** If no permissions are assigned to a user or group that the user is a member of, the user cannot access the resource.

# **Examples of Applied Permissions**



#### **Class Discussion**

The slide on this page shows two examples of assigned shared folder permissions. Examine each example and determine the applied permissions for User1.

1. Example 1 shows that User1 is a member of Groups 1, 2, 3, and 4, and that these groups have different permissions for shared Folder-A.

What are User1's effective permissions for Folder-A? FULL CONTROL

2. Example 2 shows that User1 is a member of Groups 1, 2, 3, and 4, and that these groups have different permissions for shared Folder-B.

What are User1's effective permissions for Folder-B?

NO ACCESS.

# Guidelines for Sharing Folders

- **Use Intuitive Share Names**
- **Use Names Readable by All Clients**
- Organize Disk Resources According to Security Needs

For a network to be successful, network applications, public and private data, and user home folders must be easily accessible to authorized users. When sharing folders, consider the following points:

- Use intuitive share names so that users can easily recognize and locate resources. For example, for the folder *Application*, use the share name *Apps*.
- Use share names and folder names that are readable by all client operating systems. The following table describes share and folder naming conventions.

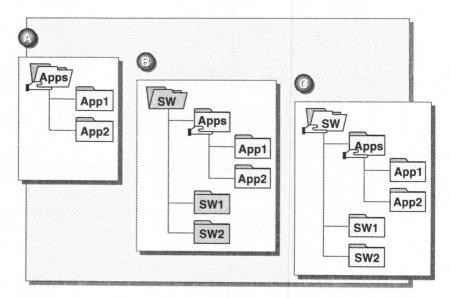
Client	Share name	Folder name
Windows NT and Windows 95	12 characters	255 characters
MS-DOS®, Windows® 3.x, and Windows for Workgroups	8.3 characters	8.3 characters

**Note** Windows NT provides 8.3 character equivalent names, but the resulting names are not intuitive to users. For example, a Windows NT folder named *Accountants Database*, would appear as *Accoun~1* to clients running MS-DOS, Windows 3.x, and Windows for Workgroups.

 Organize disk resources so that folders with the same security requirements are located within one folder hierarchy. For example, if users require Read permission to several application folders, store those folders within the same folder.

# **Examples of Shared Folders**

THE Access Permission is not on the fider, is on the share!



Based on resources stored on a server, you need to determine which folders on your servers users can and cannot access over the network. You can share any folder within a folder hierarchy. Once a folder is shared, users with the appropriate permissions have the same level of access to the contents of the shared folder, but cannot access folders that are at a higher level or at the same level as the shared folder.

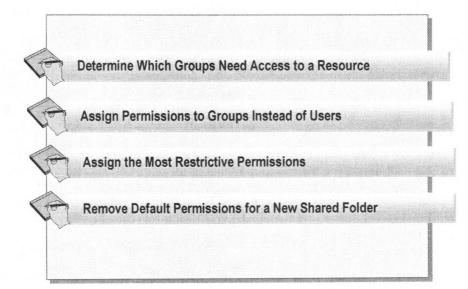
The following examples explain how to share folders to secure three folder hierarchies. In all three examples the Users group should only be able to access the contents of the Apps, App1, and App2 folders over the network.

- A. In this example, share the Apps folder and assign the Users group Read permission. Members of the Users group can connect to the Apps shared folder and will be able to read the contents of the Apps folder, which includes the App1 and App2 folders.
- B. In this example, share the Apps folder and assign the Users group Read permission. This will give users access to Apps, App1, and App2 because they are in the same hierarchy. Users will not be able to access the SW, SW1, and SW2 folders because the SW folder is in a different hierarchy.

When users connect to Apps, Apps will appears as a root folder. Users will not be able to see folders that are at a higher level or at the same level as the shared folder they are connected to.

C. In this example, share the SW folder and assign only the Administrators group Full Control permission. This will give Administrators access to SW, SW1, SW2, and Apps.

## **Guidelines for Assigning Permissions**

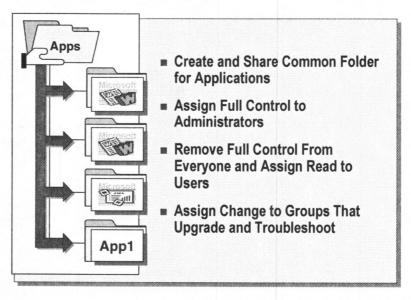


The following are general guidelines for assigning permissions to users and groups for shared folders:

- Determine which groups need access to each resource and what level of access they require. Document the groups and their permissions for each resource. For example, for the Sales Data folder, the Sales group would require Change permission; Administrators, Full Control permission; and Executives, Read permission.
- Assign permissions to groups instead of users to simplify administration.
- Add global groups to local groups, and then assign permissions to the local group.
- Assign permissions to only the groups that need access to the resource.
- Assign to a resource the most restrictive permissions that allow network users to perform required tasks.
  - For example, if users need only to read information in a folder, and they will never delete or create files, then assign the Read permission.
- Remove the default permission Everyone, Full Control from the group for a new shared folder.

**Note** When a folder is shared, the Everyone group is automatically assigned Full Control permission. For greater security, remove the Everyone group and assign permissions to the Users group. The Users group only contains accounts that you create; however, the Everyone group contains anyone who has access to your network and includes the Guest account.

# **Guidelines for Network Application Folders**



In a large networking environment, one or more servers may be dedicated to storing applications. In a small networking environment, one server may be used for both applications and data. The application folders you share will vary with each network environment.

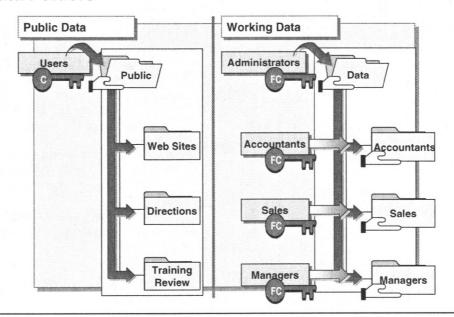
When you share application folders, consider the following points:

Create a common shared folder and organize your applications under it. For example, for applications that are not part of an application suite, create a folder named Apps. Install applications separately under the applications folder, and then share it as Apps.

Share lower-level application folders to the appropriate groups only when you need to restrict access to those folders. For example, to restrict only Accountants to Read permission for the Microsoft Excel folder, do the following:

- a. Remove permissions for the MSOffice folder for any group that contains the Accountants group or members of the Accountants group.
- b. Share the Microsoft Excel folder using the share name *Excel* and assign a local group that contains the Accountants global group Read permission.
- Assign the Administrators group Full Control permission to the Apps folder.
- Remove Full Control permission from the Everyone group and assign Read permission to the Users group. This provides more security because the Users group includes only accounts you created, whereas the Everyone group includes anyone who has access.
- Assign Change permission to groups responsible for upgrading and troubleshooting application software.

#### **Guidelines for Data Folders**



Data folders are used by network users to exchange public and working data. When sharing data folders, consider the following points.

#### **Public Data**

When you share a public folder, consider the following points:

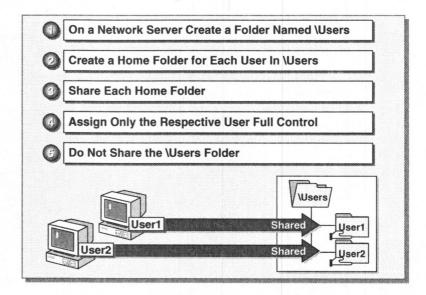
- Use centralized data folders so that data can be consistently backed up.
- Create and share a Public folder on a volume separate from the operating system and applications.
- Assign the Change permission to Users. This will provide users with a central, publicly accessible location to store and share files with others.

#### **Working Data**

When you share a data folder for working files, consider the following points:

- Create and share a Data folder on a volume separate from the operating system and applications.
  - This separates data from system and application files, and therefore streamlines backup and restore procedures. If the operating system requires reinstallation, the volume containing the data will remain intact.
- Share lower-level data folders to the appropriate groups when you need to restrict access to those folders.
  - For example, to protect data in the Accountants folder, share that folder to only the Accountants group and assign that group Change permission. Then members of the Accountants group can access the Accountants shared folder. Administrators have access by connecting to the Data shared folder.

### **Guidelines for Home Folders**



To create home folders for users on a FAT volume using only shared folder permissions to restrict access, follow these guidelines:

- 1. Create a central folder named \Users on a volume separate from the operating system and applications.
  - This streamlines backup and restore procedures. If the operating system requires reinstallation, the volume containing the home folders will remain intact.
- 2. Create a folder in \Users for each user account, with the same name as their user name. For example, for the user name Ericb, create a folder named Ericb.
- 3. On a FAT volume, share each user's home folder and assign *only* the respective user Full Control permission to his or her home folder. This guarantees privacy to the user because he or she is the only person who can connect to his or her home folder. This is the only way to protect users' folders on a FAT volume.
- 4. To specify the user's home folder, when the user logs on, in User Manager for Domains, type a universal naming convention (UNC) path in the **Home Directory To** box that includes the server name, and the %Username% variable.

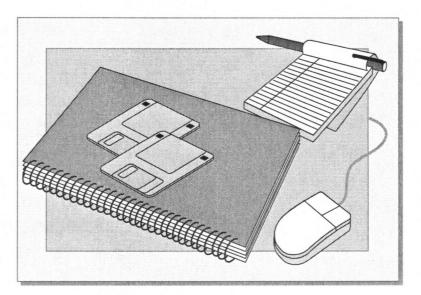
For example: \\server\_name\\Users\%\Username\%

**Note** On a FAT volume, you need to create and share home folders before you specify the home folder path in User Manager for Domains.

5. To ensure privacy, do not share the top-level folder Users.

You will be able to perform administrative tasks on home folders by logging on to the server locally, or by connecting to an administrative share (C\$, D\$, and so on).

## **Lab 7: Planning Shared Folders**



## Sharing Folders

Group Operating System Requirements
Administrators Any computer running Windows NT

Server Operators Windows NT Server domain controllers only

Power Users Windows NT Server member servers and computers running Windows NT Workstation

N.B. the root directory of workstations are all shared.

Trap drive:

11 STUDENTI \ CA\ PUBLIE

Using the Administrative Shares

Share	Purpose	
C\$, D\$, E\$	The root of each volume is automatically shared	
Admin\$	The C:\Winnt folder is shared as Admin\$	

## Requirements for Sharing a Folder

Any folder on a computer running Windows NT can be shared. The following table lists the groups and operating system requirements required to share a folder.

Group	Operating system
Administrators	Any computer running Windows NT.
Server Operators	Windows NT Server domain controllers only.
Powers Users	Windows NT Server member servers and Windows NT Workstation clients only.

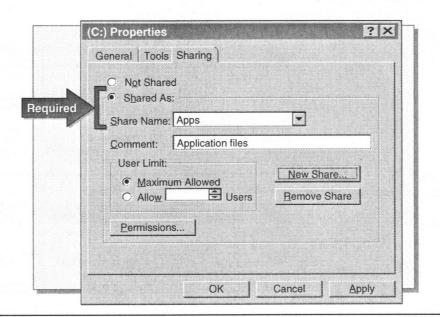
**Note** If the volume is NTFS, then the user must have at least the List permission to share the folder.

#### **Administrative Shares**

Windows NT provides the following share names used for administration.

Share	Purpose
C\$, D\$, E\$, and so on.	The root of each volume on a hard disk is automatically shared, using the drive letter appended with a dollar sign (\$). The \$ hides the shared folder from users who browse the computer. When you connect to this folder, you have access to the entire volume. You use the administrative shares to remotely connect to the computer to perform administrative tasks.
Admin\$	The C:\Winnt folder is shared as Admin\$. This is a special shared folder that is only required by the system during remote administration.

## Sharing a Folder



The first step in sharing a folder is to assign it a share name.

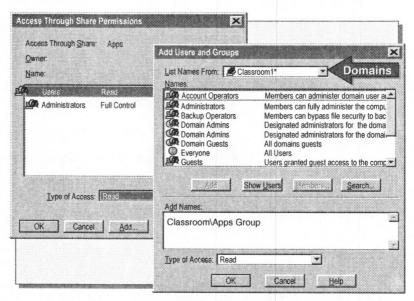
#### ► To create a shared folder

- 1. In Windows NT Explorer, right-click the folder to be shared.
- 2. Click **Sharing**. The *Folder\_name* **Properties** dialog box appears.
- 3. Configure the **Sharing** tab to include any of the following options.

Description
Provides the name remote users will use to connect to the local resource. You must enter a share name. You can create a hidden share by appending a \$ to the share name. The \$ hides the shared folder from users browsing the computer.
Provides a description for the share name. The comment appears in the <b>Map Network Drive</b> dialog box when users browse shared folders on a server. This comment should clearly identify the contents of the shared folder.
Sets the number of users that can simultaneously connect to the shared folder. The Windows NT Workstation maximum is 10. Windows NT Server is unlimited.
Sets the permissions on the folder <i>only</i> when it is accessed over the network. The Everyone group is automatically assigned Full Control permission for all new shared folders.
Appears when the selected folder is already shared. A folder can be shared multiple times with different names and permissions. However, keeping track of multiple share names requires more administration.

#### 4. Click OK.

## **Assigning Shared Folder Permissions**



After you assign a share name, the next step is to specify which users can access the shared folder by assigning permissions to selected users or groups.

#### To assign permissions for a shared folder

- 1. In Windows NT Explorer, right-click the shared folder.
- 2. Click Sharing.
- 3. In the Folder\_name Properties dialog box, click Permissions.
- 4. In the Access Through Share Permissions dialog box, click Add. The Add Users and Groups dialog box appears.
- 5. In the **Add Users and Groups** dialog box, select the user or groups that you want to assign permissions to.
- Click Show Users to display all of the user accounts in the domain. The groups and names will be added to the Add Names box.

**Note** In a multiple-domain network, click the **List Names From** arrow to reveal other domains from which you can list user and group names for assigning permissions.

- 7. In the **Type Of Access** box, click the appropriate permission for the user or group (that is, click either **No Access**, **Read**, **Change**, or **Full Control**).
- 8. Click **OK** to return to the **Access Through Share Permissions** dialog box.
- 9. Click **OK** to return to the *Folder\_name* **Properties** dialog box, and then click **OK**.

## **Modifying Shared Folders**

- Changing Shared Folder Options
- Stop Sharing Folders
- Modifying Share Names
- Modifying Shared Folder Permissions

You can modify all shared folder options on the *Folder\_name* **Properties** dialog box, except for the share name.

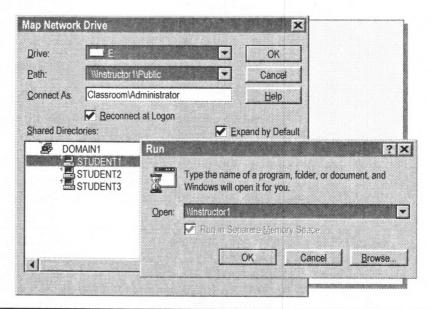
#### ► To modify a shared folder

- In Windows NT Explorer, right-click the shared folder, and then click Sharing.
- 2. On the **Sharing** tab of the *Folder\_name* **Properties** dialog box, follow the steps in the table below to complete the appropriate task.

To	Do this
Stop sharing a folder	Click <b>Not Shared</b> to stop sharing the folder, and then click <b>OK</b> . See the Important at the bottom of this page.
Modify the share	Click Not Shared to stop sharing the folder.
name	Click Apply to apply the change.
	Click Shared As, and then type in a new share name.
Modify Shared Folder Permissions	Click Permissions.
	In the <b>Access Through Share Permissions</b> dialog box, select the user or group whose permissions are to be modified.
	In the <b>Type Of Access</b> box, click the permission you want to apply, and then click <b>OK</b> .

**Important** If you stop sharing a folder when a user has a file open, the user may lose data. When you click **Not Shared**, a dialog box appears to notify you that a user is connected to the shared folder.

## **Accessing Shared Folders**



You can access a shared folder by using Windows NT Explorer or the **Run** command.

#### ► To map to a network drive using Windows NT Explorer

- 1. Start Windows NT Explorer.
- 2. On the **Tools** menu, click **Map Network Drive**, and configure the following options.

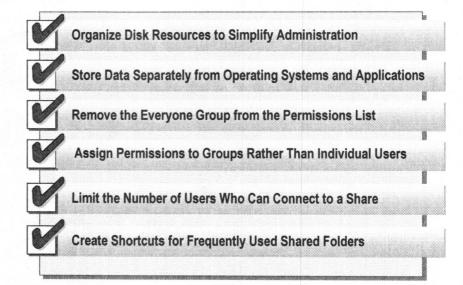
Option	Purpose
Drive	Assigns a drive letter to the shared folder so that it appears and acts like a local drive. The user can assign up to 26 letters. Drive letters that are used by local devices do not appear in the <b>Drive</b> list.
Path	Specifies the network path to the computer and the shared folder. Enter a UNC path.
Connect As	Connects to a shared folder using a different user account. For example, the administrator is at another user's computer and needs to connect to a resource that the user does not have access to. The <b>Connect As</b> option requires the domain name and the user account name in the following format: <i>Domain\User_name</i> . If there is a password on the user account, the user is prompted for it.
Reconnect at Logon	If selected, will reconnect the user to the shared folder each time the user logs on.

#### **Using the Run Command**

Using the **Run** command to connect to a network resource provides two advantages over using the **Map Network Drive** command. The advantages of using the **Run** command are as follows:

- A drive letter is not required, which conserves memory.
- The user can browse all shared folders on a computer.
- ► To access a shared folder using the Run command
- 1. Click Start, and then click Run.
- 2. In the **Open** box, type a path using the universal naming convention (UNC). The UNC format consists of the computer name and the share name for the shared folder. For example: \\server\_name\\share\_name\\

### **Best Practices**

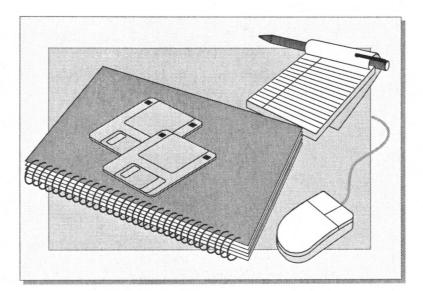


The following list provides the best practices for sharing folders:

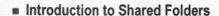
- Organize disk resources so that folders with the same security requirements are located within one folder hierarchy. This simplifies administration by streamlining how you assign permissions.
- Store data and home folders on volumes separate from the operating system and applications. This separates data files from system and application files and therefore streamlines backup and restore procedures. If the operating system requires reinstallation, the volume containing the data will remain intact.
- Remove the Everyone group from the permissions list to prevent resource access—use the local group Users instead of the Everyone group. The Users group provides more security because the group only contains accounts that you created.
- Assign permissions to groups rather than to individual users—this simplifies administration by allowing you to quickly assign permissions to multiple users at one time.
- Limit the number of concurrent users by setting the User Limit option on the Sharing tab. By doing so, you accomplish the following:
  - Enforce Concurrent Use software licensing limits.
  - Reduce network traffic for a shared folder.
- Create shortcuts for network resources that users will often connect to.

**Note** Document decisions made about shared folders and assigned permissions. Update this document when changes are made to the server, such as upgrades of software, changes to shared folder names, and assigned permissions.

## **Lab 8: Sharing Folders**



## **Review**



- **■** Guidelines for Sharing Folders
- Sharing Folders
- Accessing Shared Folders
- **■** Best Practices

- 1. How would you give a user the ability to share folders on a computer running Windows NT?

  FOWER USER

  ADITUM ISTRATOR
- 2. When a folder is shared, a user with the appropriate permissions has access to what?

  that folder & all sub-folder & all files in them
- 3. What permissions can be assigned to a shared folder?

4. What are the default permissions on a shared folder?

# Module 6: Securing Network Resources with NTFS Permissions

## Overview

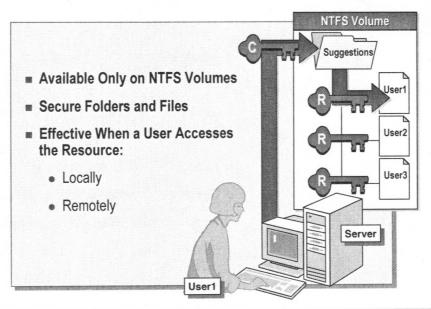
- **Introduction to NTFS Permissions**
- Combining Shared Folder and NTFS Permissions
- Guidelines for Assigning NTFS Permissions
- Assigning NTFS Permissions
- Taking Ownership of Folders and Files
- Copying or Moving Folders and Files
- Troubleshooting Permission Problems
- Best Practices

#### **Objectives**

At the end of this module, you will be able to:

- Describe the situations that require Microsoft® Windows NT® file system (NTFS) folder and file permissions.
- Define the NTFS folder and file permissions.
- Describe the result when both user and group permissions are applied to the same resource.
- Describe the result when folder permissions are different from those of the files in the folder.
- Describe the result when shared folder permissions and NTFS permissions are combined.
- Assign NTFS folder and file permissions to users and groups.
- Describe the result when files and folders are copied or moved.
- Take ownership of files and folders.
- Describe situations when it is necessary to take ownership of files and folders.
- Recognize common reasons why users cannot gain access to resources.
- Describe the best practices for administering resources with permissions.

## Introduction to NTFS Permissions



#### What Are NTFS Permissions?

NTFS permissions are permissions that are only available on a volume that has been formatted with the Windows NT file system (NTFS). NTFS permissions provide a greater degree of security because they can be assigned to folders *and* to individual files. Unlike shared folder permissions, NTFS permissions protect local files and folders, and are sometimes referred to as *local permissions*.

### Why Use NTFS Permissions?

You use NTFS permissions to protect resources from users who access the computer:

- Locally, by sitting at the computer where the resource is stored.
- Remotely, by connecting to a shared folder.

**Important** When a volume is formatted with NTFS, the Everyone group is automatically assigned Full Control permission to the volume. Folders and files created on the volume inherit this default permission.

The Shared Right is not on the folder. If someone logon locally, con use the files But not over the network!

#### **NTFS Permissions**

- Read (R)
- **₩** Write (W)
- **Execute (X)**
- Delete (D)
- Change Permission (P)
- Take Ownership (O)

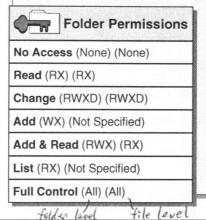
Individual NTFS permissions can be set on folders or files. The following table describes the actions that a user can take when individual permissions are assigned to a folder or file.

For a folder—a user can	For a file—a user can
Display folder names, attributes, owner, and permissions.	Display file data, attributes, owner, and permissions.
Add files and folders, change a folder's attributes, and display owner and permissions.	Display owner and permissions, change file attributes, create data in, and append data to, a file.
Display folder attributes, make changes to folders within a folder, and display owner and permissions.	Display file attributes, owner, and permissions. Run a file if it is an executable.
Delete a folder.	Delete a file.
Change a folder's permissions.	Change a file's permissions.
Take ownership of a folder.	Take ownership of a file.
	Display folder names, attributes, owner, and permissions.  Add files and folders, change a folder's attributes, and display owner and permissions.  Display folder attributes, make changes to folders within a folder, and display owner and permissions.  Delete a folder.  Change a folder's permissions.

**Note** On an NTFS volume, the person who creates a file or folder becomes the *owner*. The owner can always assign and change permissions on a file or folder.

#### **Standard Permissions**

- Are a Combination of Individual NTFS Permissions
- Give You the Ability to Assign Multiple NTFS Permissions at One Time



	File Permissions
No Acc	ess (None)
Read (F	RX)
Change	(RWXD)
Full Co	ntrol (All)

In most cases, you will use the NTFS *standard permissions*. Standard permissions are combinations of individual NTFS permissions. They simplify administration by giving you the ability to assign combinations of individual permissions at one time. Windows NT provides standard folder permissions and standard file permissions.

#### Standard Folder Permissions

The following table lists the standard folder permissions and the individual NTFS permissions that each standard permission represents.

Standard permission	Individual permissions on folders	Individual permissions on files in the folder
No Access	None	None
List	RX	Not specified
Read	RX	RX
Add	WX	Not specified
Add & Read	RWX	RX
Change	RWXD	RWXD
Full Control	All	All

#### Standard File Permissions

The following table lists the standard file permissions and the individual NTFS permissions that each standard file permission represents.

Standard permission	Individual permissions
No Access	None
Read	RX
Change	RWXD
Full Control	All

## **How NTFS Permissions Are Applied**

#### ■ Like Shared Folder Permissions

- A user's effective permissions are the combination of both the user and group permissions.
- The No Access permission overrides all other permissions
- **■** File Permissions Override the Permission for the Folder

NTFS permissions are applied to groups and users in the same way that shared folder permissions are applied.

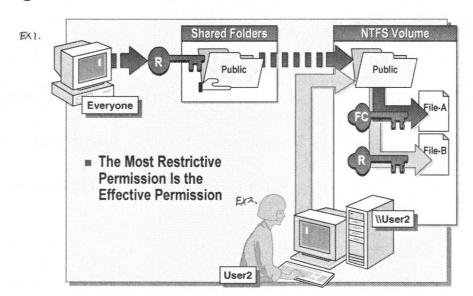
- A user can be assigned permissions directly or as a member of a group.
- A user might be a member of several groups with different permissions.

NTFS file permissions take precedence over the permissions assigned for the folder that the file is contained in. For example, if a user has Read permission to a folder and write permission to a file in that folder, then the user can write to the file.

This is also true, even when a user has No Access to a folder. The user can always access the files for which he or she has permissions by using the full UNC or local path to open the file from its respective application.

For example, if a user has No Access permission to a folder and that folder contains a file that the user has Change permission for, then the user can open the file from the file's appropriate application by typing the full path to the file in the **File Open** dialog box of the application.

## Combining Shared Folder and NTFS Permissions



To provide users with network access to disk resources, the folders containing those resources *must* be shared. Once the folder is shared, shared folder permissions are assigned to users and groups to control how they access the resource over the network. However, shared folder permissions offer limited security because they:

- Give the user the same level of access to all folders and files within the shared folder.
- Have no effect when a user accesses the resource locally.
- Cannot be used to secure individual files.

You gain the greatest degree of security by combining NTFS permissions with shared folder permissions. The most restrictive permission is always the effective permission.

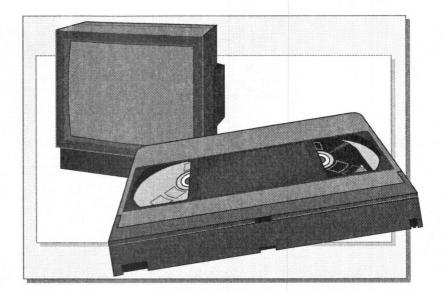
## **Examples**

In the slide example, the Everyone group has the share permission Read for the Public folder and for File-A and File-B even though Everyone has the NTFS Full Control permission for File-A because Read is the most restrictive permission.

User2 has the Full Control permission for File-A and Read for File-B. User2 is not affected by the shared folder permission assigned to Public because User2 is accessing the Public folder locally.

N.B. When combining Permission on Shared Folder from individual A group (where the individual is a member of), the less restrictive permission is used.

### **Video: Permissions**



This video shows the effective permissions when shared folder and NTFS permissions are combined.

As you view the video, watch for the answers to the following questions:

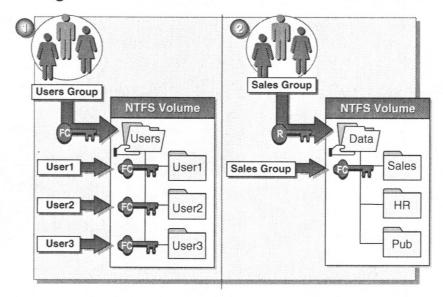
- 1. What do shared folders provide access to?

  network resources ie folder & files.
- 2. What do shared folder permissions apply to?

  folders & files & sub-folders.
- 3. What can NTFS permissions can be assigned to?

4. When you combine a shared folder permission with an NTFS permission what permission becomes the *effective* permission?

## **Examples of Combining NTFS and Shared Folder Permissions**



#### **Class Discussion**

This slide shows two examples of shared folders that contain folders or files that have been assigned NTFS permissions. Look at each example and determine a user's *effective* permissions.

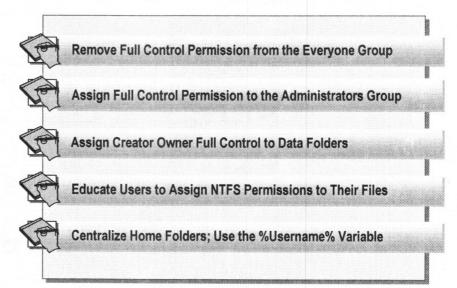
1. In the first example, the Users folder (containing home folders) has been shared, and the Users group has the share permission Full Control. User1, User2, and User3 have been assigned the NTFS permission Full Control to *only* their home folder. These users are all members of the Users group.

Do members of the Users group have Full Control to *all* home folders in the Users folder once they connect to the Users shared folder?

2. In the second example, the Data folder has been shared. The Sales group has been assigned the shared permission Read for the Data shared folder and the NTFS permission Full Control to the Sales folder.

What are the Sales group's effective permissions when they access the Sales folder by connecting to the Data shared folder?

## Guidelines for Assigning NTFS Permissions



#### **Application Folders**

When assigning NTFS permissions to application folders, consider the following:

- Remove the default permission Full Control from the Everyone group and assign it to the Administrators group. Assign groups that are responsible for upgrading and troubleshooting application software the Full Control or Change permission for the appropriate folders.
- If the applications are contained in shared folders, assign the Users group Read permission.

#### **Data Folders**

When assigning NTFS permissions to data folders, consider the following:

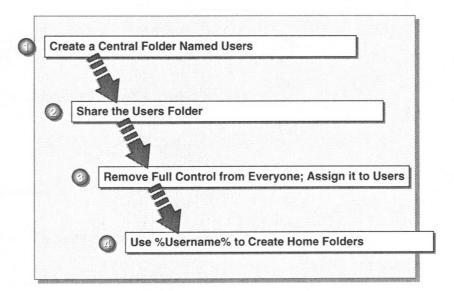
- Remove the default permission Full Control from the Everyone group and assign it to the Administrators group.
- Assign the Users group Add & Read permissions and the Creator Owner special identity Full Control permission to data folders. This gives users who log on locally the ability to delete and modify only the files and folders that they create.
- Educate users that share a computer to assign NTFS permissions to the folders and files they own.

#### **Home Folders**

When assigning NTFS permissions to home folders, consider the following:

- Centralize home folders on a network volume separate from applications and the operating system to streamline backing up data and administration.
- Use the %Username% variable to automatically assign a user's account name to the folder the NTFS Full Control permission.

#### **Home Folders**



You should store home folders on an NTFS volume on a network server. This simplifies administration by providing a central location for backing up users' data and streamlining assigning permissions.

**Tip** Educate users to store their personal and work data in their home folders. If users' home folders are stored on a network server and are moved to a different server, only the home folder path will require modification.

#### ► To create and share home folders on an NTFS volume

- 1. Create a folder named *Users* on a volume separate from the operating system and applications. If the operating system requires reinstallation, the volume containing the home folders will remain intact.
- 2. Share the Users folder to provide a single access point for network users and a single administration point for administrators.
- 3. Remove the default permission Full Control from the Everyone group and assign the share permission Full Control to the Users group.
- 4. Use the %Username% variable to automatically name home folders using users' user account names.
  - a. Start User Manager or User Manager for Domains and create a new user account or double-click an existing account.
  - b. In the New User or User Properties dialog box, click Profile, and then, in the Home Directory To box, type \\server\_name\\Users\\% Username \%

**Important** On NTFS volumes, the %Username% variable automatically assigns the Full Control permission to home folders. On FAT volumes, home folders can only be restricted by shared folder permissions.

## Assigning NTFS Permissions

- **Requirements to Assign NTFS Permissions** 
  - Owner
  - Full Control
  - Special Access: Change Permission or Take Ownership
- Default NTFS Permissions
  - The Everyone group is automatically assigned Full Control
  - New files inherit the permissions of the folder where they are created

#### **Requirements to Assign NTFS Permissions**

To assign NTFS permissions, you need to be the owner of the folder or file, or have one of the following permissions:

- Full Control
- Special Access: Change Permissions
- Special Access: Take Ownership—with this permission a user can take ownership of a file or folder, and as the owner, the user can change permissions on the resource.

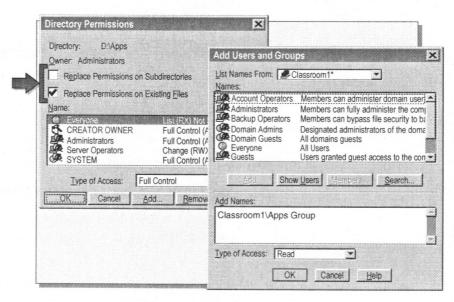
#### **Default NTFS Permissions**

The following are the default NTFS permissions:

- When a volume is formatted with NTFS, the permission Full Control is automatically assigned to the Everyone group. This gives all users with the user right to Log on Locally complete access to the volume.
- When a new folder or file is created on an NTFS volume, it inherits the permissions of the folder containing it.

**Caution** When Windows NT is installed on an NTFS volume, NTFS permissions are automatically assigned to some system folders. Do not modify the permissions on system files. For a complete list of these permissions, see *Concepts and Planning, Microsoft Windows NT Server*.

## **Assigning NTFS File and Folder Permissions**



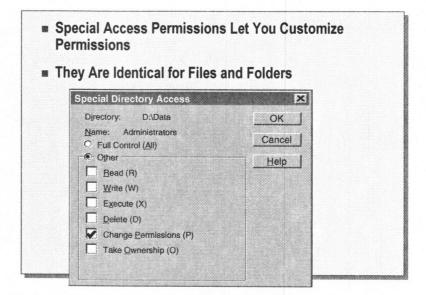
#### ► To assign NTFS permissions for files or folders

- 1. In Windows NT Explorer, right-click the folder or file, and then click **Properties**.
- 2. In the *Directory* **Properties** or *File\_name* **Properties** dialog box, click the **Security** tab, and then click **Permissions**.
- 3. In the **Directory Permissions** or *File\_name* **Permissions** dialog box, configure the following options.

Option	Purpose	
Replace Permissions on Subdirectories	If selected, changes existing permissions for <i>all</i> folders within the selected folder's hierarchy. This option does not change permissions on existing files in the folder hierarchy. This check box is <i>cleared</i> by default and is an option <i>only</i> when assigning folder permissions.	
Replace Permissions on Existing Files	If selected, changes existing permissions for all files within the <i>selected</i> folder only. It does not change file permissions for folders within the same folder hierarchy. This check box is <i>cleared</i> by default and is an option <i>only</i> when assigning folder permissions.	
Name	Displays the folder or file permissions assigned to a group or user for the resource. The first set of parentheses indicates the folder permissions, and the second set of parentheses indicates the permissions for any new files created in the folder.	
Type of Access	Displays the folder or file permissions for the selected group or user in the <b>Name</b> box and allows you to change the permission assigned to the selection.	

4. Click **Add** to add users and groups to the folder or file.

## **Assigning Special Access Permissions**



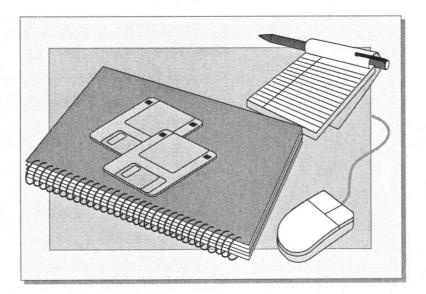
In general, standard permissions are all you need to secure folders and files. If you need to assign individual permissions, or create a custom set of permissions, then assign special access permissions. For example, to allow another user to manage permissions for files you own, assign that user the special file access permission: Change Permissions (P).

The special access permissions are identical for both files and folder.

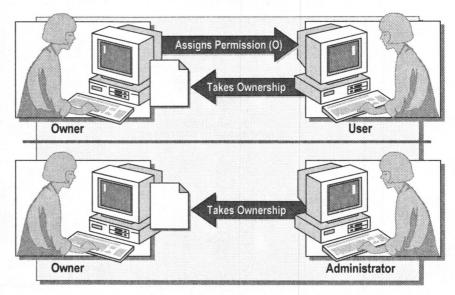
#### ► To assign special access permissions

- In Windows NT Explorer, right-click the folder or file, and then click Properties.
- 2. In the *Directory* **Properties** or *File\_name* **Properties** box, click the **Security** tab, and then click **Permissions**.
- 3. In the *Directory* **Permissions** or *File\_name* **Permissions** dialog box, select a user or group name.
- In the Type of Access list, click Special Directory Access or Special File Access.
- 5. In the **Special Directory Access** or **Special File Access** dialog box, click the appropriate permission, and then click **OK**.

## **Lab 9: Planning and Assigning NTFS Permissions**



## Taking Ownership of Folders and Files



Whoever creates a folder or file owns it. As the owner of a folder or file, a user can share the folder and assign permissions to other users and groups. A user cannot share folders or assign permissions for folders that he or she does not own. If a user has denied others access to a file and then leaves the company, you can take ownership of the file and change the permissions so that others can access the file.

#### Requirements to Take Ownership

By default, members of the Administrators group always have the ability to take ownership of a file or folder. If a member of this group takes ownership of a resource, the Administrators group becomes the resource's owner and any member of the Administrators group can access the resource.

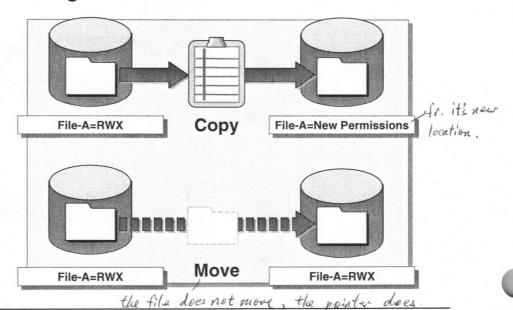
An owner cannot change the ownership of a resource they own. The owner can only give another user or group permission to take ownership of a resource. Security of the resource is thus maintained by preventing users from creating or editing files and then making them look as if they belonged to someone else.

For example, if a user assigns the No Access permission to a file, a member of the Administrators group can still take ownership of the file and make changes to it. The user, by checking the ownership of the file, would see that the administrator owned the file, and had disregarded the No Access permission on the file.

The owner can assign another group or user the *ability* to take ownership of a file or folder by assigning one of the following permissions:

- Full Control
- Special Access, Take Ownership
- Special Access, Change Permissions—with this permission, users can assign the Take Ownership permission to themselves or to another user or group.

## Copying or Moving Folders and Files



A user cannot copy or move files within or between NTFS volumes, unless the user has the correct permissions. The following table describes the required permissions to copy or move a file or folder to another folder on an NTFS volume or to another NTFS volume.

Actio n	Permission required
Сору	Add permission for the destination folder.
Move	Add permission for the destination folder and Delete for the source folder. Delete is required, because when a file or folder is moved, it is deleted from the source folder <i>after</i> it is placed in the destination folder.

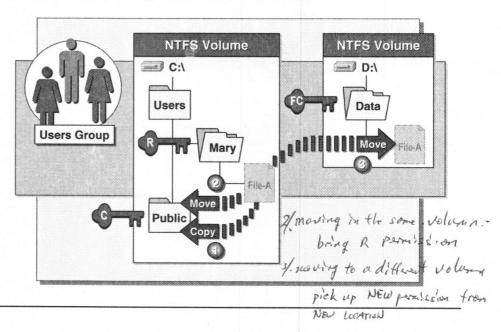
Copying and moving files or folders within and between NTFS volumes can affect the original permissions set on a file. The following table describes what happens to permissions on a folder or file when copied or moved within or between an NTFS volume.

Task	Within an NTFS volume	Between NTFS volumes
Сору	Inherits the permissions of the destination folder.	Inherits the permissions of the destination folder.
Move	Retains original permissions.	Inherits the permissions of the destination folder.

**Note** The user who copies a file or folder becomes the owner.

**Important** Files and folders that are copied or moved to FAT volumes lose their permissions, because FAT volumes do not support NTFS permissions.

## **Examples of Copying and Moving Folders and Files**



#### **Class Discussion**

In the slide example, File-A is stored in the C:\Users\Mary folder. The Users group has the following NTFS permissions to folders on drives C and D:

- Read permission for C:\Users\Mary and the files contained within it.
- Change permission for C:\Public.
- Full Control permission for D:\Data.
- 1. What permission does the Users group have to File-A after it is copied to the C:\Public folder?

charge permission

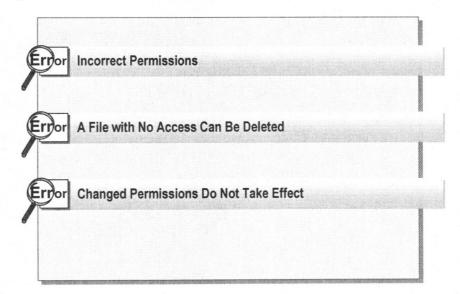
2. What permission does the Users group have to File-A after it is moved to the C:\Public folder?

READ

3. What permission does the Users group have to File-A if it is moved to the D:\Data folder?

FC.

## **Troubleshooting Permission Problems**



Troubleshooting access to network resources is a common problem. The following information provides solutions to common permission problems.

#### Problem 1

A user cannot access a resource.

#### Solution

Check the permissions assigned to the user's account and to groups to which the user is a member. If the No Access permission is assigned to the user or a group that the user is a member of, then the user has no access to the resource.

If the file was copied within an NTFS volume, or copied or moved to another NTFS volume, the file permissions may have changed by inheriting new permissions from the destination folder.

#### Problem 2

A user deletes a file, even though that user was assigned the No Access permission for the file.

#### Solution

Do not assign users the NTFS standard Full Control permission for a folder. Instead, assign users all of the individual special directory access permissions. This gives the user all of the abilities of the Full Control permission for the folder, but prevents them from deleting files in the folder (for which they have been assigned No Access).

**Note** Problem 2 is the only exception to the rule that file permissions override directory permissions. This is because Windows NT supports POSIX applications that are designed to run on a Unix file system. On the Unix file system, Write permission to a folder allows you to delete files in that folder. The NTFS Full Control permission is designed to support this feature.

#### Problem 3

You add a user to a group to give that user access to a resource, but the user still cannot access the resource.

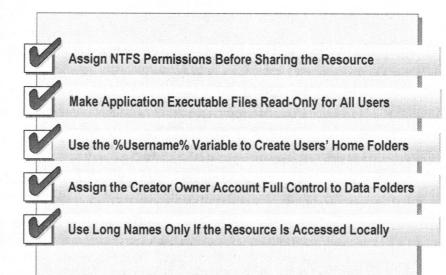
#### Solution

Ask the user to log off and then log on or ask the user to disconnect completely from the remote computer and attempt to connect again.

An object called an *access token* is created for a user every time that user logs on and is authenticated by a computer running Windows NT. The access token contains information about the groups to which the user belongs. For the access token to be updated to include the new group to which you've added the user, the user must log off and then log on again or disconnect completely from the remote computer and then reconnect.

**Note** For more information on access tokens, see the *Microsoft Windows NT Resource Kit*.

## **Best Practices**



Externall User may be using tooks with that connet use long file name.

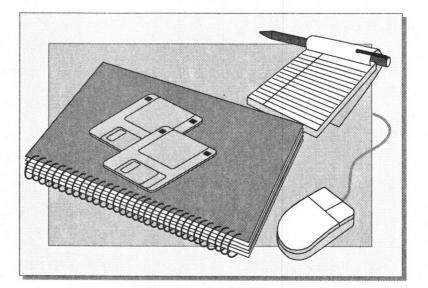
The following list provides best practices for implementing NTFS permissions:

- Assign NTFS permissions before sharing a folder. In this way, you avoid
  the issue of users connecting to and accessing folders and files before you
  fully secure them.
- Assign the Read permission to the Users and Administrators groups for all application executable files.

Damage to application files is usually a result of accidents and viruses. To prevent this type of file damage, assign the Read permission to all users, including administrators, for application executable files. By doing so, you can prevent users and viruses from modifying or deleting these files. In addition, assign the Administrators group the special access Change Permissions (P) so they can assign themselves greater access when changes to the application files are required.

- Use the %Username% variable to create home folders—this simplifies administration by automatically giving only the respective user Full Control permission to his or her home folder.
  - For clients running Microsoft MS-DOS®, use user names that are eight characters or less. Then, when the %Username% variable is used to create the home folder, the folder name can be easily read by the MS-DOS-based client.
- Assign the Creator Owner special built-in identity Full Control permission to Data folders—this gives users Full Control permission to only the files or folders that they create in the Data folder.
- Use long, descriptive names if the resource will only be accessed locally. If a folder will eventually be shared, then use folder and file names that are accessible by all client computers.

## **Lab 10: Managing Permissions**



## Review

- **Introduction to NTFS Permissions**
- **Combining Shared Folder and NTFS Permissions**
- **Guidelines for Assigning NTFS Permissions**
- Assigning NTFS Permissions
- Taking Ownership of Folders and Files
- Copying or Moving Folders and Files
- **Troubleshooting Permission Problems**
- **Best Practices**
- 1. How would you automatically create home folders to which only the individual users were assigned Full Control access?

% username %

- 2. What is the default permission once a volume is formatted with NTFS?

  NTFS every one full control
- 3. What should you always check when a user cannot access a resource?

  check which group the resource is in

convert D: Us: NTFS

## Module 7: Setting Up a Network Printer

To redirect print queue tie default printer broken), change the port the default printer using -> to apprinter,

\$ 65. t vat

net ess \$35

server

workstatton

## Overview

- **Introduction to Windows NT Printing**
- **Setting Up a Network Printer**
- Accessing a Network Printer
- **Creating a Printing Pool**
- **Setting Priorities Between Printers**
- Assigning Forms to Paper Trays
- Setting a Separator Page
- **Best Practices**

#### **Objectives**

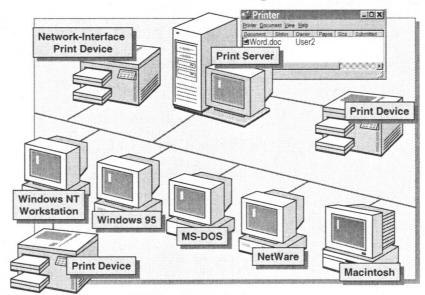
At the end of this module, you will be able to:

- Describe the requirements for printing.
- Plan how to add and share printers in your network.
- Add and share a network printer.
- Assign printer permissions to users and groups.
- Set up clients for printing.
- Connect to a network printer.
- Create a printing pool.
- Set priorities between printers.
- Schedule documents.
- Assign forms to paper trays.
- Set separator pages.
- Apply the best practices for setting up a network printer.

HP wendet Properties
General
Separator Prope
Print Processor
Print test Page.

Priter Permission - FC, monger documents, no access, Device Settings

# Introduction to Windows NT Printing



Setting up and sharing printers on a Windows NT® network requires:

 At least one computer configured as a print server, and running Windows NT Server or Windows NT Workstation. The print server is where client computers send documents to print.

The *printer* is installed on the print server. In Windows NT, a printer is the software interface between the application and the print device.

- A *print device*. In Windows NT, a print device is the actual hardware device that produces printed output.
  - A print device can be attached locally to the print server. This type of print device is referred to as a local print device.
  - If a print device has a network card, it can be attached directly to the network. This type of print device is referred to as a *network interface* print device.

Users can print from computers in the Windows NT network that are running the following operating systems:

- · Windows NT
- MS-DOS®
- NetWare

- Windows® 95
- LAN Manager 2.x
- UNIX

- · Windows for Workgroups
- OS/2

Macintosh

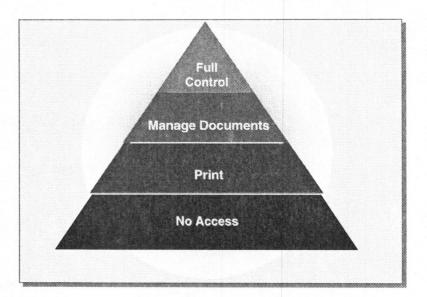
• Windows 3.1

Once a network print server is set up, you can:

- Administer a print server from any computer running Windows NT.
- Manage which print devices are available to users by controlling user permissions.
- Configure the printers.

11 Computername printername

## **Printer Permissions**



There are four levels of printer permissions: No Access, Print, Manage Documents, and Full Control. By default, all users have the Print permission.

For security reasons, you may need to limit user access to certain printers. In large organizations, you may also need to delegate printer responsibilities to one or two specific users. These types of changes are made using permissions.

The following table lists the capabilities of the four levels of permissions.

Capabilities	No Access	Print (default)	Manage Documents	Full Control
Print documents		X	X	X
Pause, resume, restart, and cancel the user's own document		X	X	X
Connect to a printer		X	X	X
Control job settings for all documents			X	X
Pause, restart, and delete all documents			X	X
Share a printer				X
Change printer properties				X
Delete printers				X
Change printer permissions				X

the print driver live on the print server. users is given a copy over

the printer

the printer

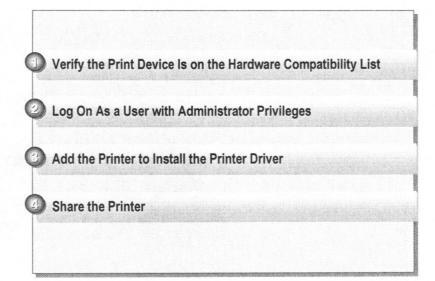
the physical printer

a printer = software on the computer which control the "print device"

printer pool = multi-piont devices BUT one printer

con hore many physical printers attach to the same machine

# Setting Up a Network Printer



Setting up a network printer makes it possible for multiple users to print to it. To set up a network printer, you need to do the following tasks:

- 1. Verify that the print device is on the Windows NT 4.0 hardware compatibility list (HCL).
  - If your print device is on the list, then Windows NT has the required printer driver.
  - If the print device is not on the list, you will need to get a printer driver from the manufacturer or use a supported driver for a print device that the unsupported print device can emulate.
- 2. Log on as a user with Administrator privileges. Members of these groups can add and share a printer. They also have the Full Control print permission and can administer printers.

A member of this group	Can administer a printer
Administrators	On any computer in the domain running Windows NT Workstation or Windows NT Server
Print Operators	On any domain controller
Server Operators	On any domain controller
Power Users	On any local computer in the domain on which the group exists

- 3. Add a printer—this installs the printer driver on the print server.
- 4. Share a printer—this allows users to connect to the printer over the network, and print to the print device connected to the printer. You can share a printer when you add it, or you can share an existing printer.

By default, the Print permission is assigned to the Everyone group.

# **Adding and Sharing a New Printer**

Use this option	То	
My Computer	Designate the computer as a print server	
Available Ports	Connect a local print device to the print server	
Manufacturer and Printers	Make sure the correct printer driver is installed	
Printer Name	Identify the printer to users who manage it	
Default Printer	Set the default printer	
Shared	Share the printer	
Share Name	Assign a share name	
Operating Systems	Make sure appropriate print drivers are available	
Test Page	Verify the printer is correctly installed	

If the print device is on the HCL, and you are logged on as a member of the appropriate group, you can add and share a printer. Users can then connect to it over the network.

### To add and share a printer

- 1. Click **Start**, point to **Settings**, and then click **Printers**. The Printers folder appears.
- 2. Double-click **Add Printer**. The Add Printer Wizard appears. The wizard steps you through adding a printer. You must decide on the following options.

Option	Use this option to	
My computer	Designate the computer as the print server the first time a printer is installed on the server. Thereafter, the selection allows you to add a printer to the print server.	
Available ports	Specify which port on the print server is attached to the local print device.	
Manufacturers, Printers	Install the correct print driver on the print server. If the driver you want is not listed, click <b>Other</b> and then provide a driver.	
Printer name	Identify the printer to the users that manage it. The name should be intuitive and descriptive of the print device.	
Default printer	Set the default printer for all Window-based applications. Then, the user does not have to set a printer for each application. This option is automatic for the first printer on the print server.	
Shared	Make it possible for users with the appropriate permission to connect to the printer over the network.	
Share name	Assign a share name. The name should tell users the type of print device or its location, and it should be compatible with all client computers on the network. The default is the printer name truncated to 8.3 characters.	

(continued) Option	Use this option to
Operating systems	Identify types of clients running Windows NT and Windows 95 that will use the printer, and to make sure that the appropriate print drivers are installed on the print server.
Test page	Print a test page to verify that the printer is correctly installed.

- 3. When you finish with the Add a Printer Wizard, click **Finish**. The **Copying Files--Files Needed** dialog box appears.
- 4. In the **Copy Files From** box, type the path to the printer driver installation files, and then click **OK**. First the **Copying Files** status box appears, and then the *printer\_name* **Properties** tab.
- 5. Click OK.

#### ► To delete a printer

- 1. In the Printers folder, click the icon for the printer that you want to delete.
- 2. Press the DELETE key.

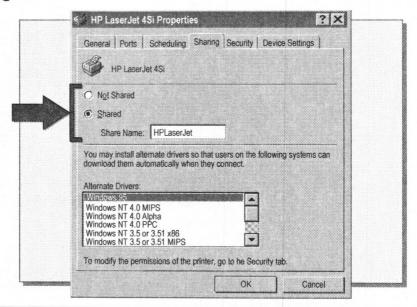
-or-

On the File menu, click Delete.

You receive a message asking you to confirm that you want to delete the printer.

3. Click Yes. The printer disappears from the Printers folder.

## **Sharing an Existing Printer**



If your network has an existing, non-shared printer, you can share it. For example, network printing increases. One user has a local print device. If you share this printer, other network users can connect to it and print to it.

#### To share a printer

- 1. Click **Start**, point to **Settings**, and click **Printers**. The Printers folder appears.
- 2. Click the icon for the printer that you want to share.
- 3. On the **File** menu, click **Sharing**. The **Sharing** tab of the *printer\_name* **Properties** dialog box appears.
- 4. Click **Shared**. A share name is assigned by default. You can type in an alternate share name.

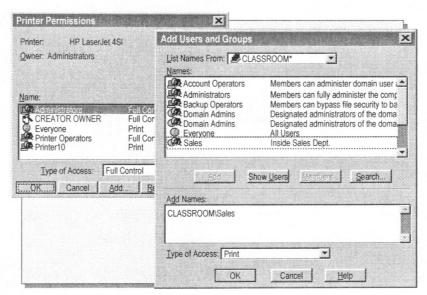
**Note** In the **Alternate Drivers** box, you can select to let other Windows NT operating systems and Windows 95 connect to the printer.

5. Click **OK**. An open hand appears under the printer icon in the Printers folder. This indicates that the printer is shared.

#### To set an existing printer as the default printer

- 1. In the Printers folder, click the icon of the appropriate printer.
- 2. On the File menu, click Set As Default.

## **Assigning Printer Permissions**



By default, the Everyone group is assigned the Print permission. If you want to restrict or expand a users printer privileges, be sure to modify the default permission.

### ► To add a user or group and assign print permissions

- 1. In the Printers folder, click the icon for the printer for which you want to change permissions.
- 2. On the **File** menu, click **Properties**.
- 3. In the *printer\_name* **Properties** dialog box, click the **Security** tab.
- 4. On the **Security** tab, click **Permissions**. The **Printer Permissions** dialog box appears.
- 5. Click Add.
  - The Add Users and Groups dialog box appears.
- 6. Select the appropriate users and groups, and then click **Add**. The user or group appears in the **Add Names** box.
- 7. In the **Type Of Access** box, click the permission you want for the user or group, and then click **OK**. The **Printer Permissions** dialog box appears.
- 8. Click OK.

## **Setting Up a Network Client**

- **Clients Running Windows NT and Windows 95** 
  - Users connect to shared printer
  - Print driver automatically copies to client computer
- **Clients Running Other Microsoft Operating Systems** 
  - · Install a printer driver locally
- Clients Running Non-Microsoft Operating Systems
  - Verify appropriate service installed on print server
  - Install a printer driver locally

#### Windows NT- and Windows 95-Based Clients

Once you have a shared printer, you do not need to do anything further for clients running Windows NT and Windows 95. The user needs only to connect to the shared printer.

#### Other Microsoft-Based Clients

For the following clients to print to a Windows NT-based shared printer, you must install a printer driver locally on the client computer.

MS-DOS	LAN Manager 2.x	Windows for Workgroups
OS/2 (with LAN Manager	Windows 3.1	
Client version 2.2c		
installed)		

#### Non-Microsoft-Based Clients

For non-Microsoft-based clients to print, you must make sure the following requirements are met:

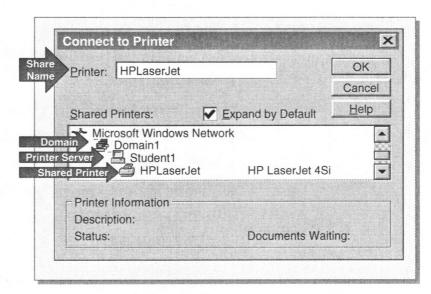
■ The print server must have a service installed on it. The following are examples of non-Microsoft-based clients and their required services.

Client computer	Service
Macintosh	Services for Macintosh
NetWare	File and Print Services for NetWare (FPNW)
UNIX	TCP/IP Line Printer Daemon (LPD) Service

You must install a printer driver locally on the client computer.

**Note** You can get the appropriate printer driver for a platform from the installation disks of each client. For more information about setting up non-Microsoft services, see the *Concepts and Planning Guide, Windows NT Server*.

# **Accessing a Network Printer**



The default print permission for all users is Print, which makes it possible for them to access a network printer. The interfaces that different clients use vary.

## Clients Running Windows NT 4.0 and Windows 95

Clients running Window NT 4.0 and Windows 95 use the Printers folder to connect to a shared network printer. When they first connect, the appropriate printer driver is automatically installed into client memory. Thereafter, Windows NT-based clients and Windows 95-based clients behave differently.

- Each time a Windows NT-based client reconnects, if the printer driver is not current, a copy of the new driver is downloaded. This automatically keeps the printer driver current.
- The printer driver in the Windows 95-based client is not automatically kept current. If you update the driver on the print server, you must manually install the driver on the Windows 95-based client.

#### To connect to a printer

- 1. In the Printers folder, double-click the Add Printer icon. The Add Printer Wizard appears.
- 2. Click **Network Printer Server**, and then click **Next**. The **Connect to Printer** dialog box appears.
- 3. In the **Printer** box, type the UNC name of the printer you want to connect to.

-or-

In the **Shared Printers** box, select the UNC name of the printer you want to connect to.

In the **Shared Printers** box, all the domains in the network appear.

a. Double-click a domain.

The computers and the shared printers in that domain appear in the **Shared Printers** box.

- b. Click a shared\_printer.
- 4. Click **OK**. The Add Printer Wizard appears.
- 5. Click **Yes** to use this as the default printer, or **No** if you do not want to use it as the default printer. Then, click **Next**.
- 6. Click Finish. The printer\_name Properties tab appears.
- 7. Click OK.

**Note** Windows version 3.1 and Windows for Workgroups clients use Print Manager to connect to a printer.

### Other Clients

To connect to a printer from clients running operating systems other than Windows NT and Windows 95, use the commands specific to the clients.

■ For LAN Manager clients running MS-DOS or OS/2, use the **net use** command.

**net use lpt**x \\server\_name\\sharename

■ For NetWare clients configured with a Monolithic IPX and NetWare VLM, use the NetWare Capture command.

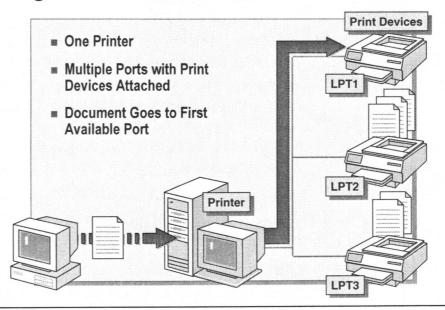
capture queuename

For UNIX clients running TCP/IP, use the LPR utility.

lpr -Sserver\_name -Psharename filename

For the Apple Macintosh, use Chooser.

# **Creating a Printing Pool**



A printing pool is one printer connected to multiple print devices through multiple ports of the print server. They are useful in a network with a high volume of printing. They decrease the time that documents wait in the print queue. For you, it is easier to manage one printer than multiple printers.

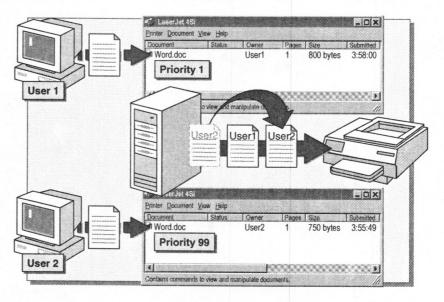
The user prints a document without having to find out which print device is available. The printer checks for an available port. It checks the ports in the order that they are added, so add the port for the quickest print device first.

#### ► To create a printing pool

- 1. In the Printers folder, select the icon for the appropriate printer.
- On the File menu, click Properties.
   The printer\_name Properties dialog box appears.
- 3. Click the **Ports** tab.
- 4. Select the Enable printer pooling check box.
- 5. Select the ports that you want to add, and then click **OK**.

**Best Practice** Locate the printing devices in a printing pool in close proximity, so that users do not have to search several locations for their documents.

# Setting Priorities Between Printers



Setting priorities between printers makes it possible for you to set priorities between groups of documents. For example, all documents from executives print before other users, or critical documents always print before lower priority documents.

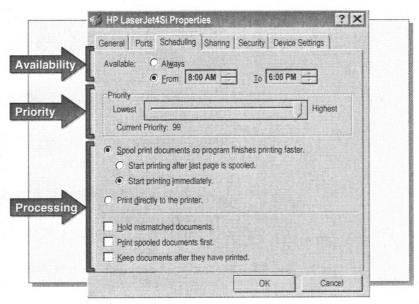
Setting priorities between printers requires that you do the following:

- Connect two or more printers to the same print device. These printers must:
  - Be on the same print server.
  - Use the same port to connect to the print device. The port can be either a
    physical port on the print server or the UNC name of a network printer.
- Set a different priority for each printer connected to the print device. Then
  users print to the different printers. For example, executives print to the
  highest priority printer.

Notice the graphic above. User1 sends documents to a printer with the lowest priority of 1, while User2 sends documents to a printer with the highest priority of 99. User2's documents will always print before User1's.

Setting a printer priority is part of scheduling documents, which is presented in the next section.

## **Scheduling Documents**



Scheduling documents gives you flexibility in setting up how documents print. A schedule change affects all the documents that are sent to the printer. The following are the different tasks that you can schedule and when you might use the tasks.

Task	Situation	
Set available printing times	Large documents print at night so that they will not monopolize the printer during the work day.	
Set priorities between printers	Critical documents always print first.	
Change how the printer processes documents	Large documents start printing immediately, before they are completely processed.	

#### **▶** To change scheduling options

- 1. In the Printers folder, select the icon for the appropriate printer.
- 2. On the **File** menu, click **Properties**. The *printer\_name* **Properties** dialog box appears.
- 3. Click the **Scheduling** tab. Notice, the default for available hours is Always.
- 4. In the **Available From** box and the **To** box, type or select the hours you want the documents to print, and then click **OK**.
  - Changing the time determines when a document prints, but not when it processes.
- 5. Under **Priority**, move the slider to the priority that you want. The default is the lowest priority, which is 1. The highest priority is 99.

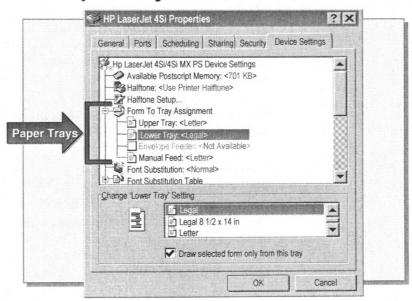
6. Select the option buttons or check boxes that you want for the following processing options.

Options	Description	
Spool print documents so program finishes printing faster	Either this option or the <b>Print directly to the printer</b> option is selected. If you choose this option, the documents will spool. This option has two choices.	
•Start printing after last page is spooled	A document will not print until completely spooled. The application that is printing is unavailable during the spooling.	
•Start printing immediately	A document starts to print before it spools completely, which means that it prints sooner. The application that is printing is available sooner.	
Print directly to the printer	The document does not spool, which decreases printing time. Select this option only for a non-shared printer.	
Hold mismatched documents	Documents that do not match the configuration of the printer will not print. This stops incorrect documents from printing.	
Print spooled documents first	A spooled document prints before a partially spooled document.	
Keep documents after they have printed	Documents remain in the print spooler after printing, and can be quickly resubmitted for printing.	

**Important** In Windows NT printing, there is a *spooler* on the print server. The spooler processes and schedules documents. *Spooling* is the process of storing documents on the hard disk, and then sending them to the printer.

7. Click **OK**. Windows NT changes the settings.

# **Assigning Forms to Paper Trays**



If a print device has multiple trays that hold different types of forms, you can assign a form to a paper tray. Users can then select the form from within their application. When they print, the print job will be routed to the correct paper tray. Form refers to the paper size and type. Examples of forms are:

Legal size

• Envelopes #10

Note size

Letter small

#### ► To assign a form type to a paper tray

- 1. In the Printers folder, select the icon for the appropriate printer.
- 2. On the **File** menu, click **Properties**. The *printer\_name* **Properties** dialog box appears.
- 3. Click the **Device Settings** tab.

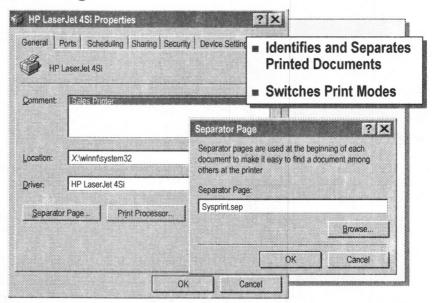
In the top window, below **Form to Tray Assignment**, click the paper tray that you want to assign the form to. Notice, the **Change** *paper\_tray* **Setting** appears in the bottom window.

**Important** The default form setting for a paper tray is Not Available.

- 4. Click a paper size. The paper size appears next to the selected paper tray in the top window.
- 5. Click OK.

**Note** Once you have set up a paper tray, users specify the form they want from within an application. Windows NT knows in which paper tray the form is located.

# **Setting a Separator Page**



Separator pages have two functions, which are:

- To identify and separate printed documents.
- To switch print devices between the different print modes, as shown in the following table. Print modes process documents into a format that the print device understands.

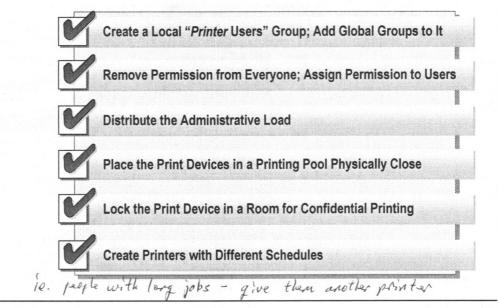
Windows NT includes three separator page files. They are located in the \(\systemroot\\System32\) directory.

File name	Function	
Sysprint.sep	Prints a page before each document. Compatible with PostScript printing devices.	
Pcl.sep	Switches the printing mode to PCL for HP-series printing devices and prints a page before each document.	
Pscript.sep	Switches the printing mode to PostScript for HP-series printing devices, but does not print a page before each document.	

#### To set up a separator page

- 1. In the Printers folder, select the icon for the appropriate printer.
- 2. On the **File** menu, click **Properties**. The *printer\_name* **Properties** dialog box appears. The **General** tab is active.
- 3. Click Separator Page. The Separator Page dialog box appears.
- 4. In the **Separator Page** box, type the name of the separator page file, or click **Browse** and select the file that you want, and then click **Open**.
- 5. Click **OK**, and then click **OK** again.

## **Best Practices**

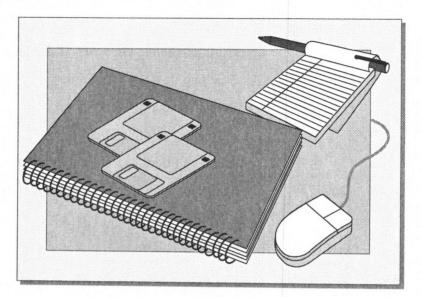


The following list provides best practices for setting up a network printer:

- Use the same guidelines that apply to any shared resource. Create a local "printer Users" group with Print permissions and then put global groups into the local group.
- Remove the Print permission from the default group Everyone. Instead assign the Print permission to the built-in group Users. This will limit printer use to those users in the domain for which you have created accounts.
- Distribute the administrative load. If security is not an issue, assign a user the Manage Documents or Full Control print permission, or add a user to the Print Operators group to manage the printer.
- Secure the print device in a locked room if it is used for confidential information. Let only members of the Administrators group manage the printer.
- For printing pools, place the print devices physically close to each other. Then users do not have to check separate locations for their printed documents.
- Create multiple printers with different schedules to reduce printer traffic during peak hours. Have users send large documents, such as accounting reports, to a printer that is available only at night so that those documents will wait to print during non-working hours.

**Tip** Document network printers and assigned permissions. This will help you keep track of changes made to network printers by other users who manage printers.

# Lab 11: Setting Up a Network Printer



## Review

- **Introduction to Windows NT Printing**
- Setting Up a Network Printer
- Accessing a Network Printer
- Creating a Printing Pool
- Setting Priorities Between Printers
- Assigning Forms to Paper Trays
- Setting a Separator Page
- **Best Practices**
- 1. What is the difference between a printer and a print device?
- 2. What is the default print permission for users?
- 3. You have added and shared a printer. What do you do to set up clients running Windows NT 4.0 so they can print, and why?
- 4. What is the highest priority you can assign to a printer?
- 5. Why would you create a printing pool?

# Module 8: Administering Network Printers

## Overview

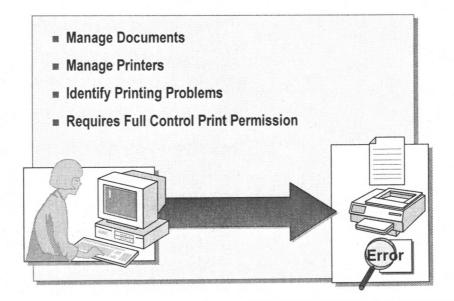
- Introduction to Administering Printers
- **■** Deleting a Document
- Setting a Notification, Priority, and Printing Time
- Pausing, Resuming, and Purging a Printer
- Redirecting Documents
- **Taking Ownership of a Printer**
- **Identifying Printing Problems**

## **Objectives**

At the end of this module, you will be able to:

- Describe how documents are printed.
- Delete a document.
- Set a notification for a document.
- Set the printing time for a document to print.
- Pause and resume a printer.
- Purge all the documents in a printer.
- Redirect documents to a different printer.
- Take ownership of a printer.
- Identify printing problems.

# ◆ Introduction to Administering Printers



You can administer network printers locally or remotely over the network. Administration tasks include:

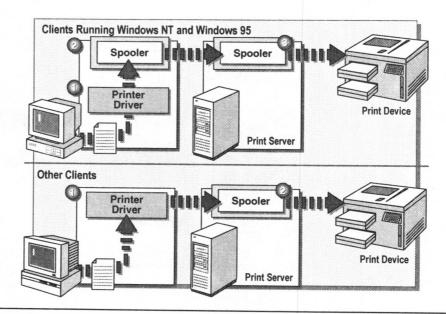
- Managing documents, which includes the following tasks:
  - Delete a document
  - Set a notification

- Change a document priority
- Set a print time for a document
- Managing printers, which includes the following tasks:
  - Pause and resume a printer
  - Redirect documents
- Purge a printer
- · Take ownership of a printer
- Identifying printing problems.
- The requirement for administering printers is the Full Control print permission. Members of the Administrators, Print Operators, Server Operators, or Power Users groups have this permission.

The table describes the rights and built-in print capabilities of the Printer Operators, Server Operators, and Power Users groups.

Group	Built-in capabilities	
Print Operators and Server	Add and remove printers	
Operators	Share printers	
	Take ownership of a printer	
Power Users	Add and remove printers	
	Share printers	
	Take ownership of a printer	

## **How Documents Print**



Having an overview of the printing process helps you in managing a printer. For example, in Windows NT® there is a *spooler* on the print server, which processes and schedules documents for printing. If a document becomes stuck in this spooler, you might need to stop and restart the spooler using Control Panel Services.

## Windows NT- and Windows 95-Based Clients

Windows NT- and Windows 95-based clients have an additional spooler on the client computer. After a user sends a document to print, the following occurs:

- 1. The printer driver partially processes the document to an acceptable format for the print device.
- 2. The document goes to the spooler on the client computer where it stays until there is room in the spooler on the print server.
- 3. The print server spooler finishes processing the document. The document waits in the spooler until a print device is available. Then, it prints.

## **Other Clients**

For the other client computers there is only a spooler on the print server. After the user sends a document to print, the following occurs:

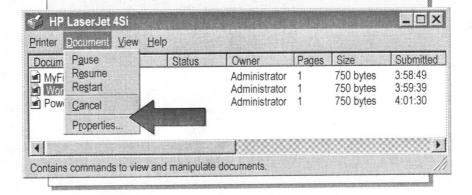
- 1. The printer driver completely processes the document to an acceptable format for the print device.
- 2. The document waits in the spooler until a print device is available. Then, it prints.

**Note** For non-Microsoft-based clients, the appropriate service must be running on the print server.

# **Deleting a Document**



**■ Use the Cancel Command** 



You may need to delete a document before it prints. For example, if the document has the wrong printer settings, delete it before it prints incorrectly.

To delete other users' documents, a user must have the Full Control or Manage Document permission. Users with the Print permission can delete their own documents.

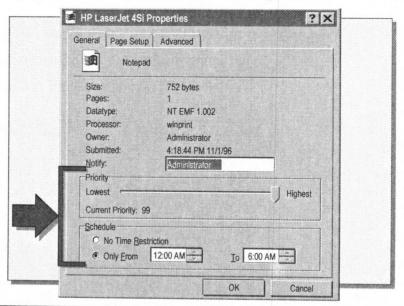
#### ► To delete a document using the DELETE key

- 1. Click **Start**, point to **Settings**, and then click **Printers**. The Printers folder opens.
- 2. Double-click the appropriate printer icon. The *printer\_name* dialog box appears.
- 3. Click the appropriate document, and then press the DELETE key. The document disappears from the *printer\_name* dialog box.

#### ► To cancel a document

- 1. In the Printers folder, double-click the appropriate printer icon. The *printer\_name* dialog box appears.
- Select the appropriate document, and then on the **Document** menu, click Cancel.

# Setting a Notification, Priority, and Printing Time



You can control print jobs by setting the notification, priority, and printing hours. To set the notification, priority, and printing hours for a document, a user must have the Full Control or Manage Document print permission for the appropriate printer.

## ► To set a notification, priority, and printing time

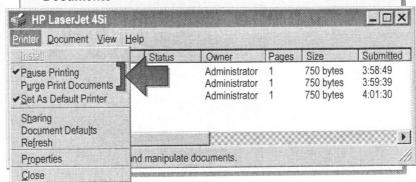
- 1. In the Printers folder, double-click the appropriate printer icon. The *printer\_name* dialog box appears.
- 2. Select the document for which you want to make a change.
- 3. On the **Document** menu, click **Properties**. The *document\_name* **Properties** dialog box appears with the **General** tab active.
- 4. Click the appropriate command as indicated in the following table.

To	Do this	Situation
Set a notification	In the <b>Notify</b> box, type the logon name of the user who is to receive the notification.	Change the print notification, when someone other than the user who printed the document needs to retrieve it.
Change a document priority	Move the slider to the priority you want. The highest priority is 99 and the lowest is 1.	Change a priority so that a critical document prints before other documents.
Set available print hours	In the <b>Only From</b> and the <b>To</b> boxes, change the hours to when you want the document to print.	Set night hours for a large document that takes a long time to print. This allows you to make sure that it spools correctly during work hours, but that it prints at night.

5. Click OK.

# Pausing, Resuming, and Purging a Printer

- **Select Pause Printing to Pause All Printer Documents**
- **Cancel the Pause Printing Selection to Resume Printing**
- Select Purge Print Documents to Delete All Printer Documents



Pausing, resuming, and purging a printer may be necessary if there is a printing problem.

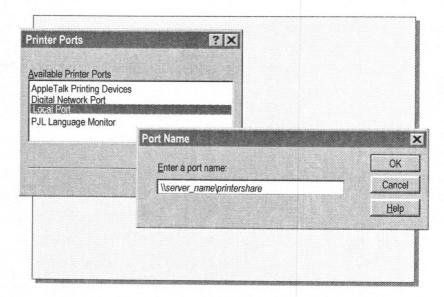
#### ► To pause, resume, or purge a printer

- 1. In the Printers folder, double-click the appropriate printer icon. The *printer\_name* dialog box appears.
- 2. On the Printer menu, click the appropriate command.

To	Do this	Situation
Pause a printer	Click Pause Printing. A check mark appears in the menu next to Pause Printing.	Pause the printer if there is a problem with the print device.
Resume a printer	Click Pause Printing. The check mark next to Pause Printing disappears.	Resume printing when a non- operational print device is repaired.
Purge a printer	Click <b>Purge Print Documents</b> . All documents disappear from the <i>printer_name</i> window.	Purge a printer if you need to delete all documents, such as old documents in the spooler.

**Note** You can quickly pause a printer by taking the printing device offline.

# **Redirecting Documents**



You can redirect documents to either a local or network print device. For example, if a printer is connected to a faulty print device, redirect the documents so users do not need to resubmit them.

When adding a network port, you can only add an existing port. You cannot create, delete, or configure ports over the network. You must do this locally.

To redirect documents locally, add a port connected to a local print device. This is the same procedure as adding local ports to set up a printing pool.

## ► To redirect documents over the network

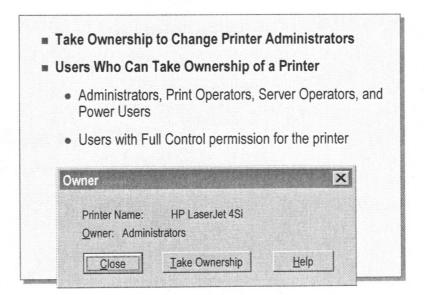
- 1. In the Printers folder, select the appropriate printer icon.
- 2. On the **File** menu, click **Properties**. The *printer\_name* **Properties** dialog box appears.
- 3. Click the **Ports** tab. The **Ports** tab displays the current configuration of the ports.
- 4. Click **Add Port**. The **Printer Ports** dialog box appears, listing the available printer port types.
- 5. Click **Local Port**, and then click **New Port**. The **Port Name** dialog box appears.
- 6. In the **Enter a port name** box, type the UNC name of another printer—for example, \\prntsrv4\\HPLaser4

The new printer must use the same print device driver as the current printer.

You may need to remove the original port to ensure the documents print to the redirected port. When there are multiple ports, the printer searches for an available port in the order that the ports were added.

7. Click OK.

# **Taking Ownership of a Printer**



Taking ownership of a printer lets you change printer administrators. By default, the user who installed the printer owns it. If that user can no longer or should no longer administer the printer, you should take ownership of it—for example, if the current owner leaves the company.

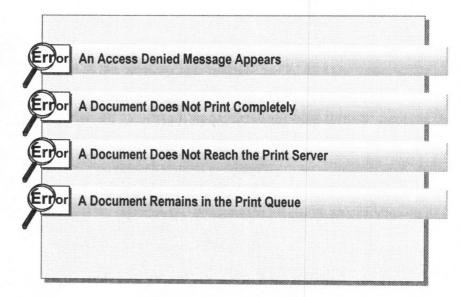
The following users can take ownership of a printer:

- By default, members of the Administrators, Print Operators, Server Operators, and Power Users groups.
- A user or a member of a group that has been granted the Full Control permission for the printer.

#### ► To take ownership of a printer

- 1. In the Printers folder, select the appropriate printer icon.
- 2. On the **File** menu, click **Properties**. The *printer\_name* **Properties** dialog box appears.
- 3. Click the **Security** tab.
- 4. On the Security tab, click Ownership. The Owner dialog box appears.
- 5. Click **Take Ownership**. The **Security** tab appears.
- 6. Click **OK**. Windows NT changes the ownership of the printer to your user account.

# **Identifying Printing Problems**



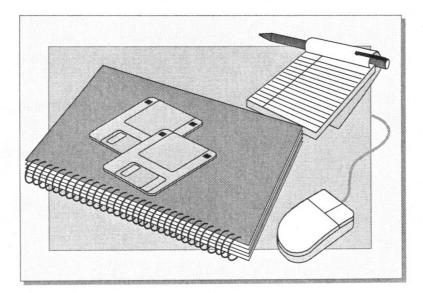
The following table describes common printing problems and their solutions.

Problem	Possible cause	Solution
User receives an Access Denied message when trying to configure a printer from an application (for example, Microsoft Excel).	The user does not have the appropriate permission to change printer configurations.	Change the user's permission, or configure the printer for the user.
The document does not print completely or comes out garbled.	Incorrect printer driver installed.	Change the current driver.
The hard disk starts thrashing and the document does not reach the print server.	Insufficient hard disk space for spooling.	Create more free space, or move the spooler location to another partition.
No one can print to the server. There are documents on the server that will not print and that you cannot delete.	Stalled print spooler.	Start Control Panel Services, stop the spooler service, and then restart it.

#### To determine the cause of a problem

- 1. Check that the print device is operational. Determine if some users can print normally.
- 2. Check that the printer matches the print device.
- 3. Check that the print server is operational and that there is enough disk space to spool.
- 4. Verify that the client has the correct printer driver.

# **Lab 12: Managing Documents and Printers**



# **Review**

- **Introduction to Administering Printers**
- Deleting a Document
- Setting a Notification, Priority, and Printing Time
- Pausing, Resuming, and Purging a Printer
- Redirecting Documents
- Taking Ownership of a Printer
- Identifying Printing Problems
- 1. When a Windows NT-based client prints, where on the client does the document wait until there is room on the print server? Where does it go on the print server?
- 2. Why would you need to take ownership of a printer?
- 3. What print permission does a user need to change the priority on another user's document?
- 4. Which software components do you check if a user's documents do not print?

# Module 9: Auditing Resources and Events

## Overview

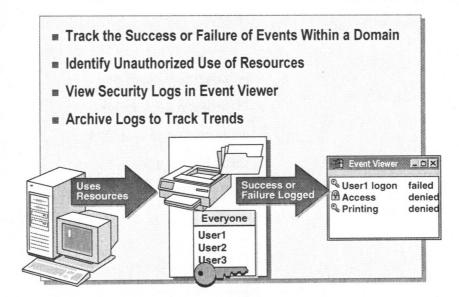
- **Introduction to Auditing**
- Planning an Audit Policy
- Implementing an Audit Policy
- **Using Event Viewer**
- **Best Practices**

## **Objectives**

At the end of this module, you will be able to:

- Plan an audit policy and determine which events to audit.
- Set up an audit policy for the domain using User Manager for Domains.
- Set up auditing on files and directories using Windows NT® Explorer.
- Set up auditing on printers using menu options in the Printers group.
- View and archive security logs using Event Viewer.
- Apply best practices for auditing resources and events.

# Introduction to Auditing



Windows NT auditing is used to track user activities and system-wide events on a network. Through auditing, you can specify that an action or event be written to a security log. The audit entry shows the following:

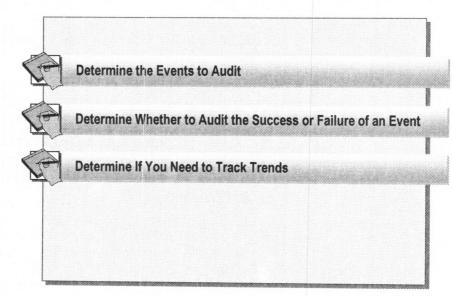
- The action performed
- The user who performed the action
- The date and time of the action

You use the audit policy to select the types of security events that will be recorded for a domain. The events will then appear in the security log of the domain controllers. The security log becomes your tool for tracking the events you specify.

On a computer running Microsoft® Windows NT Workstation, or on a computer running Windows NT Server that is not a domain controller, the audit policy affects only the security log of that computer.

- You can set up one audit policy for a domain to:
  - Track the success and failure of events, such as when users log on, an
    attempt by a particular user to read a specific file, changes to users and
    groups, and changes to the security policy.
  - Eliminate or minimize the risk of unauthorized use of resources.
- You use Event Viewer to view audited events that have been recorded in the security log.
- You can archive log files to track trends over time. This is useful to determine use of printers or files, and to verify attempts at unauthorized use of resources.

# **Planning an Audit Policy**



When planning an audit policy, consider the following:

- Determine events to audit, such as:
  - Use of file and directory resources
  - Users logging on and off
  - When Windows NT Server is shut down and restarted
  - User and group changes
  - Security policy changes such as assignment of privileges or logon capabilities
- Determine whether to audit the success and/or failure of events. Tracking the success of events can tell you how often specific files or printers are accessed. You can use this information in resource planning. Tracking the failure of events will alert you to possible security breaches.

In medium and high security networks, you should track:

- The success and failure of users logging on.
- The use of resources.
- Determine if you need to track trends. If so, you should plan on archiving event logs.

**Note** Too much auditing can create excess overhead on the system. If your server is heavily used, you may need to keep auditing to a minimum.

Car Save event log.

# Implementing an Audit Policy

- An Audit Policy Is Set on a Computer-by-Computer Basis
- **Auditing Requirements** 
  - Only Administrators can set up auditing
  - Server Operators can view and archive logs
  - Files and directories must be on NTFS volumes only
- Auditing Process
  - Set the auditing policy
  - Specify the events to audit for files, directories, and printers

An audit policy is set on a computer-by-computer basis. For example, to audit events that occur on the primary domain controller, such as user logon and changes made to user accounts, you must set the audit policy on the primary domain controller. To audit events on any other computer in the domain, such as access to a file on a member server, you must set an audit policy on the member server.

Events are recorded in the local computer's security log, but can be viewed from any computer by a user with administrative privileges to the computer where the events occurred.

## **Auditing Requirements**

The following are the requirements to set up and administer auditing:

- Only Administrators can set up auditing for files, directories, and printers on domain controllers.
- To set up auditing on a computer that is not a domain controller, you must be in the Administrators group on that computer.
- By default, the user right *Manage Auditing and Security Log* is only granted to the Administrators group.
- Members of both the Administrators and Server Operators groups can view and archive security logs and perform other administrative tasks once auditing has been set up.
- You can only audit files and directories on NTFS volumes.

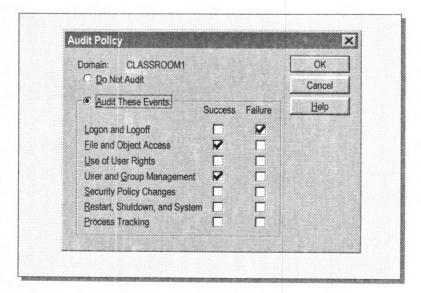
## **Auditing Process**

Setting up auditing is a two-part process:

- Set the audit policy and select the events to audit.
- Specify the events to audit for files, directories, and printers.

Policy is set I live in each machine.

# **Defining an Audit Policy**



The first step to implementing an audit policy is to select the events to audit.

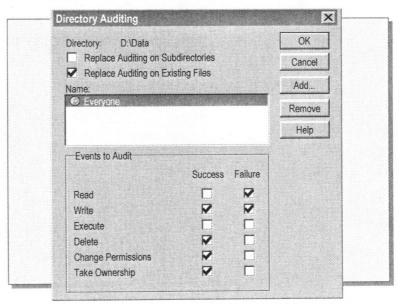
#### ► To enable auditing for the domain

- 1. Start User Manager for Domains.
- 2. On the Policies menu, click Audit. The Audit Policy dialog box appears.
- 3. Click **Audit These Events**, and then select the appropriate **Success** and **Failure** check boxes.

Description
A user logged on or off, or made or broke a network connection to a server or to the local server.
A user accessed a directory, file, or printer that is set for auditing. This event must be selected to audit file or print resources.
A user exercised a right (except those rights related to logging on and logging off).
A user account or group was created, changed, or deleted. A user account was renamed, disabled, or enabled, or a password was set or changed.
A change was made to the user rights, audit, or trust relationships policies.
A user restarted or shut down the computer, or an event has occurred that affects system security or the security log (for example, the audit log fills up and entries are discarded).
Detailed tracking information for various events, such as program activation.

4. Click **OK** when you are finished.

## **Auditing Files and Directories**



If you want to audit individual files or directories, you must specify what events you want audited.

#### ► To set up auditing on files or directories

- 1. Start Windows NT Explorer, and then select the file or directory to audit.
- 2. On the File menu, click Properties.
- 3. Click the **Security** tab.
- 4. Click Auditing.

The File Auditing or Directory Auditing dialog box appears.

5. For directory auditing, by default, auditing changes apply only to the directory and its files. Make the following selections as needed.

Do this	If you want to	
Select the Replace Auditing on Subdirectories check box.	Have auditing changes apply to the files in subdirectories as well.	
Click to clear the <b>Replace Auditing</b> on Existing Files check box.	Apply auditing changes to the directory only.	

6. Click Add.

The Add Users and Groups dialog box appears.

7. Select the appropriate domain, users, and groups. Then, click **Add**, and then click **OK**.

**Important** If you audit the Everyone group instead of the Users group, you can track the use of a resource by anyone who connects to it, not just the users you have created accounts for in the domain.

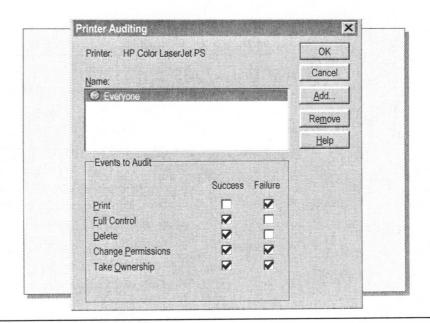
8. Under **Events to Audit**, select the event successes and failures that you want to audit.

<b>Audit this</b>	
event	To track
Read	On files, the display of file data, attributes, permissions and owner.
	On directories, the display of file names, attributes, permissions, and owner.
	Audit Read for all sensitive data.
Write	On files, changes to file data or attributes, and display of permissions and owner.
	On directories, the creation of directories and files, changes to attributes, display of permissions, and owner.
	Audit Write for all sensitive data.
Execute	On files, the display of attributes, permissions, and owner; and running of program files.
	On directories, changing directories, and display of attributes, permissions, and owner.
	Audit Execute in high security environments.
Delete	Deleted files or directories.
	Audit Delete for all sensitive data and in medium and high security environments.
Change	Changes to file or directory permissions.
Permissions	Audit Change Permissions in medium and high security environments.
Take	Changes to file or directory ownership.
Ownership	Audit Take Ownership in medium and high security environments.

Click **OK** to return to the **Properties** dialog box.
 Click **OK**.

- ► To remove file or directory auditing for a user or group
- Select the name of the user or group, and then click **Remove**.

## **Auditing a Printer**



When you audit printer usage, like when you audit files and directories, you must specify the events that you want audited.

#### ► To set up auditing on a printer

- 1. Click Start, point to Settings, and then click Printers.
- 2. Select the printer that you want to audit.
- 3. On the File menu, click Properties, and then click the Security tab.
- 4. Click Auditing. The Printer Auditing dialog box appears.
- 5. Click Add. The Add Users and Groups dialog box appears.
- 6. Select the appropriate domain, users, and group, click **Add**, and then click **OK** to return to the **Printer Auditing** dialog box.

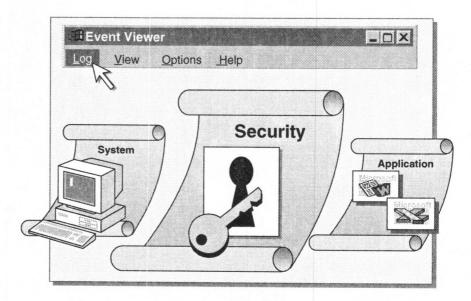
Notice that the Events to Audit selections no longer appear dimmed.

7. Under Events to Audit, select the event successes and failures that you want to audit.

Audit this event	To track
Print	Printer usage. This is useful for billing individual departments.
Full Control	Changes to job settings, pausing, restarting, moving or deleting documents, sharing a printer, or changing printer properties. This is useful in high security environments.
Delete	Deleted print jobs. This is useful in high security environments.
Change Permissions	Changes to printer permissions. This is useful in medium and high security environments.
Take Ownership	Changes to printer ownership. This is useful in medium and high security environments.

8. Click OK.

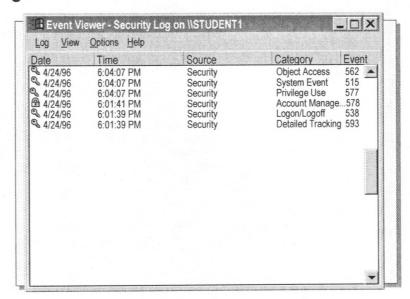
# Using Event Viewer



Event Viewer provides information about errors, warnings, and success or failure of a task. This information is stored in one of threeypes of logs:

- System—contains errors, warnings, or information generated by Windows NT. Selection of events is preset by Windows NT.
- Security—contains information about the success or failure of audited events. The events that are recorded are a result of your audit policy.
- Application—contains error, warnings, or information generated by programs, such as a database or e-mail program. Selection of events is preset by the program developer.

## **Viewing Security Logs**



#### ► To view the security log on the local computer

- 1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Event Viewer**. The default system log appears.
- 2. On the Log menu, click Security.

Successful events appear with a key icon; unsuccessful events appear with a lock icon. Other key information includes the date and time that the event occurred, and the category of the event. The **Category** indicates the event, such as **Object Access** or **Account Management**.

3. To view additional information for any event, select the event, and then on the **View** menu, click **Detail**.

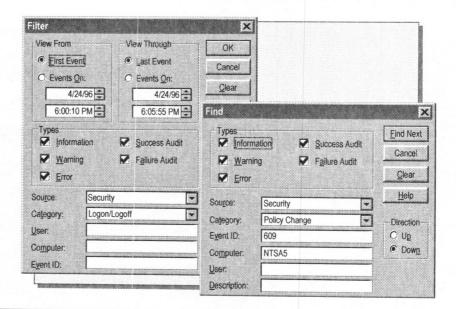
**Note** If your computer is connected to the selected computer by a modem, select the **Low Speed Connection** check box.

#### To view the security log on a remote computer

- 1. On the Log menu, click Select Computer.
  - The Select Computer dialog box appears.
- 2. In the **Computer** box, type the name of the remote computer, or double-click the domain and select the computer from the list.

**Note** To view a computer in another domain, the appropriate trust relationship must exist, and your Domain Admins group must exist in the local Administrators group of the domain or computer for which you want to view the log.

## **Locating Events**



When you first start Event Viewer, all events recorded in the selected log appear automatically. You can change what appears in the log, making it easier to locate specific events using the **Filter Events** command. You can search for information using the **Find** command.

#### **▶** To filter or find events

- 1. Start Event Viewer.
- 2. On the View menu, click Filter Events.

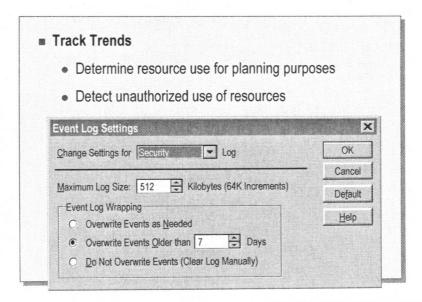
-or-

On the View menu, click Find.

3. Select the filtering or find criteria.

Option	Description
View From/ View Through	Filter only: Specify the dates for which you wish to view events.
Types	Select the types of events that you want to view.
Source	Specify the software or component driver that logged the event
Category	Select the classification of the event as defined by the source; for example, a security log category is Logon/ Logoff.
User	Specify a user account to locate events resulting from a specific user.
Computer	Specify a computer name to locate events resulting from a specific computer.
Event ID	Shows an event number to identify the event. This number helps product support representatives track events.
Description	Find only: Specify text that would appear in the description of the event.
Click OK.	

## **Archiving the Security Log**



You can track trends in your system by archiving event logs. Viewing trends helps you determine resource use and plan for growth. You can also determine a pattern if unauthorized use of resources is a problem.

## **Event Log Settings**

When you select events to audit, you need to keep in mind that the log can become full, which makes it unable to record any more events; however, you can avoid this problem. In the **Event Log Settings** dialog box, you can control:

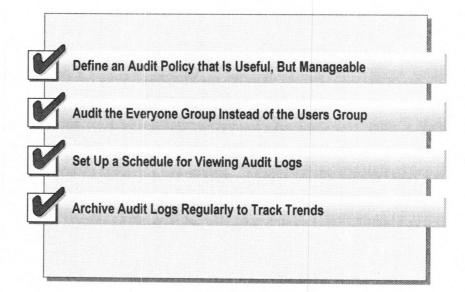
- The size of the logs you choose to archive:
  - Logs can be from 64K to 4,194,240K.
  - The default is 512K.
- How events are recorded, by selecting any of the following options:
  - Overwrite Events as Needed
  - Overwrite Events Older than x Days: enter the number of days
  - Do Not Overwrite Events: requires you to clear the log manually
     If you select Do Not Overwrite Events, you may need to archive the
     information in the current log before you clear it.

#### ► To archive, clear, and view an archived log

- 1. In Administrative Tools, start Event Viewer.
- 2. On the **Log** menu, configure the following commands.

To	On the Log menu	
Archive the security log	Click Save As, and then type a file name.	
Clear a log	Click <b>Clear All Events</b> . This will create a security log entry stating that the log was cleared.	
View an archived log	Click <b>Open</b> , and then type the name and path to the log.	

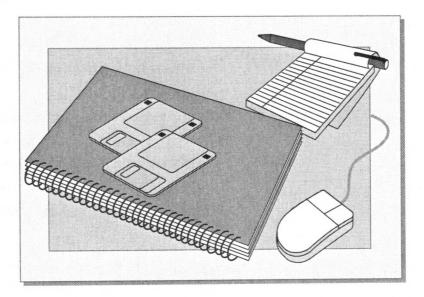
## **Best Practices**



The following list provides best practices for auditing resources and events:

- Define an audit policy that is useful, but manageable. Audit only those events that will provide you with meaningful information about your network environment. This will minimize usage of server resources and make key information easier to locate.
  - In minimum and medium security environments, track successful events if you need to determine resource usage. In a high security environment, track all successful events.
  - In minimum and medium security environments, track unsuccessful events to alert you to possible security breaches. In a high security environment, track all unsuccessful events.
  - Always audit sensitive and confidential data.
- Audit the Everyone group instead of the Users group. This will ensure that anyone who can connect to network is audited, not just the users you create accounts for in the domain.
- Set up a schedule for viewing audit logs. Make it a regular part of your network administration tasks.
- Archive audit logs regularly to track trends. This is useful for determining resource use for planning purposes.

# **Lab 13: Auditing Resources and Events**



## **Review**

- **Introduction to Auditing**
- **Planning an Audit Policy**
- **Implementing an Audit Policy**
- Using Event Viewer
- **Best Practices**

- 1. On which computer would you have to set an audit policy to audit domain logons?
- 2. On which computer would you have to set an audit policy to audit a directory located on a computer running Windows NT Workstation that is part of the domain?
- 3. What event must be set in the **Audit Policy** dialog box before you can audit files, directories, and printers?
- 4. Who can set up auditing? Who can administer auditing?

# Module 10: Monitoring Network Resources

## Overview

- Introduction to Monitoring Network Resources
- Monitoring Computer Properties
- Setting Administrative Alerts
- Sending Messages to Users
- **Viewing a System Configuration**
- **Best Practices**

## **Objectives**

At the end of this module, you will be able to:

- Describe the situations that require monitoring network resources.
- Use Server Manager to monitor server usage.
- User Server Manager to view server properties.
- Set administrative alerts.
- View system configuration information.
- Describe the best practices for monitoring network resources.

## **Introduction to Monitoring Network Resources**

#### Why Monitor Network Resources?

Assess and manage server resource usage

#### Server Manager

- Provides a graphical view for viewing and managing resource usage
- Requires membership in Administrators or Server Operators group

#### **■ Windows NT Diagnostics**

 Provides a graphical view of the operating system configuration and computer hardware

## Why Monitor Network Resources?

You monitor network resources to assess and then manage resource usage on network servers. For example, you can see if a user is connected to a file that another user is trying to access. You can then send a message to the user who is connected to the file and let the user know that someone else needs to access the file.

## Server Manager

Server Manager gives you the ability to view the properties of both local and remote computers by performing the following tasks:

- View a list of connected users.
- View and administer shared resources.
- View open resources.
- Send messages to connected users.
- Create a list of users that will receive Windows NT system alerts.

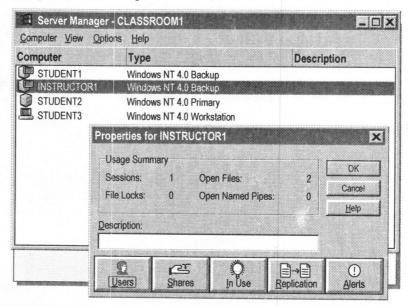
The following table describes the requirements for using Server Manager.

# A member of these groups Administrators or Server Operators for the selected domain Administrators or Power Users for the selected computer Can administer The servers and workstations in the selected domain. Member servers or workstations.

## **Windows NT Diagnostics**

Windows NT® Diagnostics provides a graphical interface to view computer hardware and operating system information. It is used to gather information to help troubleshoot hardware and memory problems.

# Monitoring Computer Properties



#### ► To start Server Manager

- Click Start, point to Programs, point to Administrative Tools, and then click Server Manager. The following information appears in the Server Manager window for the current domain:
  - The computer name and the operating system and version it is running.
  - An icon indicating whether the computer is a domain controller, a server, or a workstation.
  - If a computer is not running, the icon for the computer appears dimmed.
  - A description (configured by the user).

**Tip** You can view all computers in the domain that are running Windows NT, view just the servers, or view just the workstations, by clicking the appropriate option on the **View** menu.

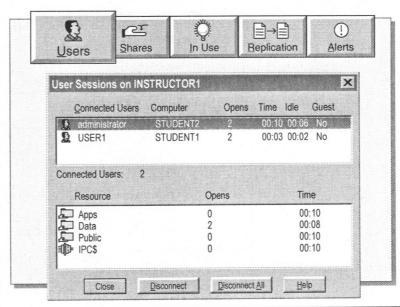
#### **▶** To view computer properties

- To view computers in another domain, on the Computer menu, click Select Domain.
- 2. Double-click the computer name to view its properties. The following table describes the information for the selected computer in the **Properties for** *computer\_name* dialog box:

Item	Description
Sessions	The number of users remotely connected to the computer.
<b>Open Files</b>	The number of shared resources opened on the computer.
File Locks	The number of file locks by users on the computer.
<b>Open Named Pipes</b>	The number of named pipes opened on the computer.

3. Click the appropriate button to view user connections and resources in use.

## **Monitoring User Sessions**



The Users button provides information on user sessions. You can:

- View users connected over the network to the computer, and view the shared folders that they are connected to.
- View the files opened by each user.
- Disconnect users from the computer.

This information is useful in determining which users you should contact when you need to stop the Server service to perform a backup or restore operation, and which users you should contact when another user is trying to access a file that is already in use.

#### **▶** To view user sessions

In the Properties for computer\_name dialog box, click Users. The following table describes the information under Connected Users.

Item	Description
Connected Users	The user name of a connected user.
Computer	The name of the computer where the user is logged on.
Opens	The number of resources the user has open on this computer.
Time	The time elapsed since this session was established.
Idle	The time elapsed since the user last accessed the resource.
Guest	Whether this user has guest status on the computer.

When you select a user, the shared resources to which the user is connected appear under **Resource**, including the name of the resource, the number of files the user has open, and the time elapsed since the resource was first opened.

IPC+ - Inter- process

#### **Disconnecting Users**

You can disconnect one or all connected users to:

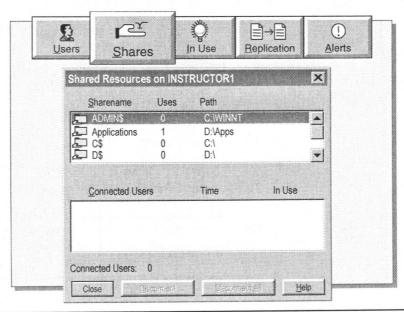
- Immediately apply changes made to group memberships, and to shared folder and NTFS permissions.
- Free idle connections on a computer running Windows NT Workstation.
   Windows NT Workstation allows only 10 incoming network connections.
- Shut down a server.

#### **▶** To disconnect users

To disconnect one user, select the user, and then click **Disconnect**.
 To disconnect all users, click **Disconnect All**.

**Caution** Always notify users that a server will be out of service, and make sure that no files are open when the Server service is stopped or the server is shut down; otherwise, users may lose data.

## **Monitoring Shared Resources**



The **Shares** button provides a list of shared resources on the computer and the users that are connected to each resource. Use this button to:

- Determine if the maximum number of users that are permitted to access that resource has been reached. This may be one reason why a user cannot connect to a shared resource.
- Disconnect users. If users turned off their computers without either logging off or disconnecting from the network resource, their connection may still be active.

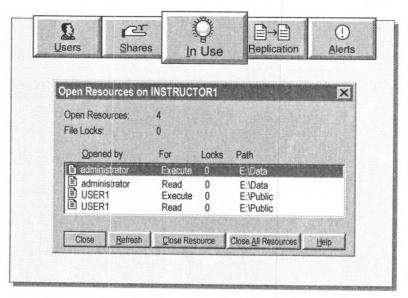
**Caution** Always notify users before disconnecting them from a resource or they may lose data.

#### ► To view shared resources

In the Properties for computer\_name dialog box, click Shares. The
following table describes the information in the Shared Resources on
computer\_name dialog box.

Item	Description
Sharename	The name of the shared resource. This could be a shared folder, a printer, or a named pipe.
Uses	The number of connections to the shared resource.
Path	The path of the shared resource.
Connected Users	The names of the users connected to the selected shared resource.
Time	The time elapsed since the user first connected to this resource.
In Use	Whether the user currently has any files open from this shared resource.

## **Monitoring Resources in Use**



The **In Use** button provides a list of the users that are connected to a shared resource and the files that they have open. Use this button to:

- Determine if a file is in use. For example, if a user cannot access a specific file because the file is open by another user, you can notify the user of the file that another user needs to access the file.
- Close a file. For example, if you make changes to NTFS permissions for a file, for those changes to be immediately effective, the file has to be closed and then reopened.

#### ► To view resources in use

 In the Properties for computer\_name dialog box, click In Use. The following table describes the information in the Open Resources on computer\_name dialog box.

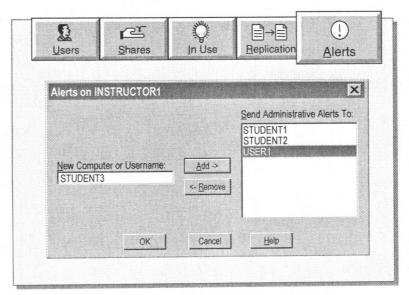
Item	Description
Open Resources	The total number of open resources (files, printers, or named pipes) on the computer.
File Locks	The total number of file locks on open resources.
Opened by	The user name of the user who opened the resource.
For	The permissions granted when the resource was opened.
Locks	The number of locks on the resource by that user.
Path	The path of the open resource.

2. Click **Refresh** to update the list of open resources. This box does not update automatically.

#### ► To close a resource

■ To close a single resource, select the resource, and then click **Close** Resource. To close all resources, click **Close All Resources**.

# **Setting Administrative Alerts**



The **Alerts** button is used to create a list of users or computers that should receive an alert when there are Windows NT operating system problems, such as security and access problems, user session problems, and printer problems. For example, you would want the Administrators group to be notified when there is a power loss on a particular computer so that appropriate action can be taken.

### ► To configure computers and users to receive administrative alerts

- 1. In the Properties for computer\_name dialog box, click Alerts.
- 2. In the New Computer or Username box, type a computer or user name.
- 3. Click **Add** to add the computer or user name to the **Send Administrative Alerts To** box.
- 4. Click OK.

**Note** Alerts are generated *only* by the Windows NT Alerter service. They are not generated by application programs.

# **Sending Messages to Users**

- Send Messages to Alert Users of a Disruption in Service or Resource Availability
  - Performing a backup or restore operation
  - · Disconnecting users from a resource
  - Upgrading software or hardware
  - Shutting down the server
- Start Server Manager, and then Select the Computer
- On the Computer Menu, Click Send Message
- **Type the Message, and then Click OK**

You should always send messages to all users connected to a particular computer when there will be a disruption to the server or the resource availability. The following are common reasons for sending messages to users:

- Performing a backup or restore operation
- Disconnecting users from a resource
- Upgrading software or hardware
- Shutting down the server
- ► To send a message to all users connected to a computer
- 1. Start Server Manager.
- 2. In the Computer column, select the appropriate computer.
- 3. On the **Computer** menu, click **Send Message**. The **Send Message** dialog box appear.
- 4. Type your message, and then click **OK**.

**Note** The Messenger service must be running to send messages. It is started by default. Computers running Windows® 95 must be running WinPopUp.exe to receive messages.

# **Viewing a System Configuration**

#### ■ The Windows NT Diagnostics Tool Is Used to:

- Gather information about hardware and memory for both local and remote computers
- Print detailed reports for technical support

The Windows NT Diagnostics tool is used to gather information about a computer's hardware and software configuration and to provide a graphical interface for you to view and print the configuration.

#### **▶** To start Windows NT Diagnostics

 Click Start, point to Programs, point to Administrative Tools, and then click Windows NT Diagnostics.

The following table describes the types of information that you can view.

Item	Description
Version	Operating system information, including version numbers, build and service pack information, and the identity of the registered owner.
System	ROM BIOS and CPU information, including the CPU type and the number of CPUs in the computer.
Display	Information about the video driver and adapter.
Drives	Available drives and their types, including removable (floppy or optical), non-removable (hard disk), and remote (network connections).
Memory	Information about physical and virtual memory. Specifics about the paging file location, total memory, available memory, and a memory load index are displayed.
Services	Services listed in the <b>CurrentControlSet</b> , along with a state or status of running or stopped.
Resources	Active devices and details about each resource, including direct memory access (DMA), interrupt (IRQ) status, memory, and port information.
	IRQ interrupts within the computer and which device has locked a particular interrupt for use.
	DMA channels that are used by devices or drivers.
	(This list supports sorting.)

Item	Description
Environment	Environment variables for the process environment (same as typing set at a command prompt), system, and user environment.
Network	Network-related configuration information, including current network statistics.

**Note** To view and print the diagnostics for another computer in a multiple domain environment, on the **File** menu, click **Select Computer**.

## **Printing a Report**

You can create a report for a specific tab or for all of the tabs.

#### ► To print and save a report

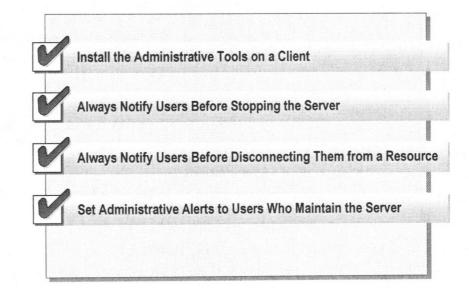
1. On the File menu, click Print Report.

The following table describes the available print options.

Click	To
Scope	Print the information on the current tab or on all tabs.
<b>Detail Level</b>	Print a summary or detailed report.
Destination	Print the information to a file, the Clipboard, or the default printer.

2. On the File menu, click Save Report.

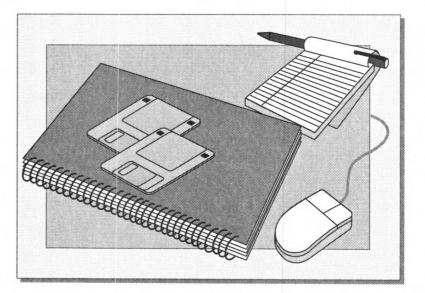
## **Best Practices**



The following list provides best practices for monitoring network resources:

- Install the Windows NT Server Administrative Tools on a client computer running Windows NT Workstation or Windows 95 client (from the \Clients\Srvtools folder on the Windows NT Server compact disc). This allows you to administer any computer running Windows NT Server from the client.
- Always notify users before stopping the server. Users may lose data if you shut down the server while they have a file open.
- Always notify users before disconnecting them from a resource. Users may lose data if they are disconnected from the server when a file is open.
- Set administrative alerts to users (and their computers) responsible for maintaining the server.

# **Lab 14: Monitoring Network Resources**



## **Review**

- **Introduction to Monitoring Network Resources**
- Monitoring Computer Properties
- Setting Administrative Alerts
- Sending Messages to Users
- Viewing a System Configuration
- **Best Practices**

- 1. What tools are used monitor network resources?
- 2. What computer properties can you manage with Server Manager?
- 3. What is the difference between the **Alerts** option and the **Send Message** command?
- 4. What tool can you use to create a hardware configuration report?

# Module 11: Backing Up and Restoring Data

## Overview

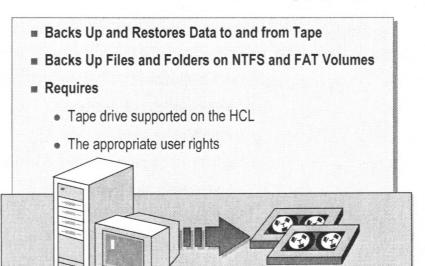
- Introduction to the Windows NT Backup Program
- Planning a Backup Strategy
- Backing Up Data
- Scheduling a Backup Using a Batch File
- **Implementing a Restore Strategy**
- Restoring Data
- **Best Practices**

## **Objectives**

At the end of this module, you will be able to:

- Describe the requirements for backing up and restoring data.
- Plan a backup strategy.
- Prepare the network for a backup.
- Perform a backup to tape.
- Use a batch file and Microsoft® Windows NT® At Scheduler to schedule backups.
- Select the best strategy to restore files and folders.
- Restore backup data onto a computer from a tape.
- Apply the best practices for backing up and restoring data.

## Introduction to the Windows NT Backup Program



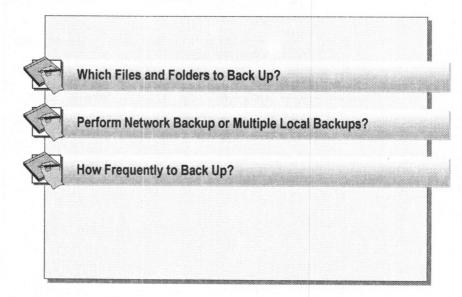
The Microsoft® Windows NT® Backup program is a graphical tool used to back up data from and restore data to NTFS or FAT volumes. You can either perform backups manually or schedule an unattended backup.

To back up and restore data:

- The tape drive must be supported on the hardware configuration list (HCL).
- The user must have the appropriate user right.
  - All users can back up any files and folders for which they have the Read permission.
  - To back up all files and folders, a user must have the Backup Files And Directories user right.
  - To restore all files and folders, a user must have the Restore Files and Directories user right.
  - Members of the Backup Operators or Server Operators groups have these right.

**Note** Windows NT Backup is not intended for a volume recovery; it does not back up data at the sector level. Also, Windows NT Backup only supports backing up to tape. To back up information to floppy disks or other non-tape media, use the Microsoft MS-DOS® **xcopy** or **backup** commands.

# Planning a Backup Strategy



Before you begin backing up data, you need a backup strategy that meets the needs of your organization, and guarantees the recovery of lost data. There is not a right or wrong strategy. Consider the following:

- Which files to back up—there is a general backup rule: if you cannot get along without it, back it up.
- Whether to perform a network backup or multiple local backups—this
  depends on which computers your organization uses for storing critical data.
  - Do a network backup when the critical data is on multiple servers or you want to perform a backup over the network.

Advantages	Disadvantages		
Backs up the entire network.	Users must copy their important files to the servers.		
Requires fewer tape drives.	Cannot back up the Registry on remote computers.		
Less media to manage.	Increases network traffic.		
One user can do the backup.	Requires greater planning and preparation.		

Do multiple local backups when the critical data is on client computers.

Advantages	Disadvantages
Fewer network resources	Requires more tape drives and tapes.
committed.	Users are responsible for backing up the data on
	their computers. The users may not be reliable.

 Do both network and local backups when the critical data is on servers and workstations.

- How frequently to back up—this depend on the following:
  - How critical the data is to your company. You would want to back up critical data more often.
  - How frequently the data changes. If users create or modify reports only on Fridays, a weekly backup for the report files would be sufficient.

**Best Practice** Plan to perform backups when network usage is low. If files are in use, Windows NT only backs up the last saved version of the file.

## **Determining Which Files and Folders to Back Up**

- Always Back Up
  - Critical files and folders
  - The Registry on a BDC or PDC
- Periodically Back Up
  - Files that rarely change
- Never Back Up
  - Temporary files

Use the following guidelines to help you determine which files and folders to back up.

- Always back up:
  - Critical files and folders your organization needs to operate.
  - The Registry on any domain controller, a BDC or PDC. Each domain controller maintains a copy of the directory database, which is stored in the Registry. Backing up the Registry on a domain controller prevents loss of all user accounts and security information.

**Important** Windows NT Backup can only back up the Registry on the computer where the tape drive is installed. If possible, you should have your tape drive installed on a domain controller.

- Periodically back up files that seldom change or are not critical to your organization.
- Do not back up temporary files, as they change constantly and are rarely used to recover data.

## **Determining the Backup Type to Use**

Type	Backs Up	Marker
Normal	All selected files and folders	Yes
Сору	All selected files and folders	No
ncremental	Selected files and folders if changed since the last backup	Yes
Differential	Selected files and folders if changed since the last backup	No
Daily Copy	Files and folders that changed during the day	No

attribute

Windows NT Backup provides five backup types, which are also called backup methods. An effective backup strategy might combine these types.

This backup type	Backs up	
Normal	Selected files and folders, and marks their archive attributes.	
Сору	Selected files and folders, and does not mark their archive attributes.	
Incremental	Selected files and folders, and marks their archive attributes, but only those files which have changed since the last time the files were backed up and marked.	
Differential	Selected files and folders, but only files which have changed since the last time they were backed up and marked. Does not mark their archive attributes.	
Daily copy	Only those files and folders that have changed during that day. Does not mark their archive attributes.	

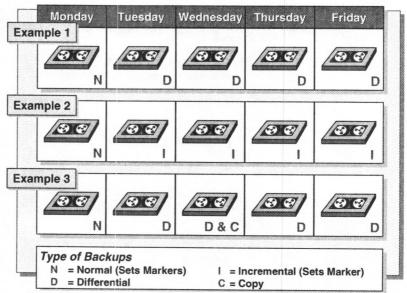
#### **Backup Markers**

Windows NT Backup can set a backup marker, also known as the archive attribute. The marker indicates that the file has been backed up, which affects incremental and differential backups.

For example, you perform a differential backup on Tuesday and Wednesday. The Wednesday backup includes the files backed up on Tuesday, even if they did not change. This is because the first differential backup did not set backup markers. The second differential backup is cumulative.

Tip Because the copy backup type does not mark files as backed up, use it to make tape copies that will not interfere with ongoing backups, for example, an archive tape.

# **Examples of Using Different Backup Types**



You can combine backup types. Some backup types require more time to back up data, but less time to restore. Others require less time to back up, but more time to restore. You need to consider where you want to spend your time. The following are some examples.

#### **Example 1: Normal and Differential Backups**

Monday is a normal backup and Tuesday through Friday are differential backups that do not set markers. Each differential backup backs up all changes since Monday. If data is corrupted on Friday, you only need to restore the Monday and Thursday backups. This strategy takes more time to back up but less time to restore.

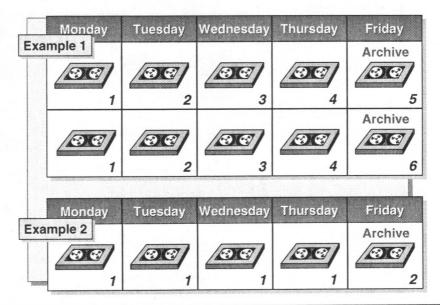
## **Example 2: Normal and Incremental Backups**

Monday is a normal backup and Tuesday through Friday are incremental backups that set markers. Each incremental backup only backs up changes since the previous day. If data becomes corrupted on Friday, you would need to restore all backups beginning with Monday. This strategy takes less time to back up but more time to restore.

## Example 3: Normal, Differential, and Copy Backups

This strategy is the same as Example 1 except that there is a copy done on Wednesday. Because a copy does not set markers, it does not interrupt the usual backup schedule. This is helpful when you need to send data to someone. For example, perform a copy when you need to send financial information to a Comptroller.

## **Rotating and Archiving Tapes**



Another issue to consider when developing your backup strategy is tape rotation. Rotating tapes means reusing them. This is a common practice that lowers the cost of backups.

You may want to archive some tapes. Archived tapes are useful for maintaining a record of data for a specific date and time, for example, a quarterly record of financial data in case of an IRS audit. When you archive a tape, you remove it from the tape rotation.

The following are two examples of tape rotation.

#### Example 1

Each day of the week is on a different tape. The tape for one day of the week is archived and removed from rotation. In this example, it is the tape for Friday.

For the following weeks, use the Monday through Thursday tapes for the same day of the week, for example, put the Monday backup on the Monday tape. These backups could either replace or append the previous backup on the tape.

#### Example 2

The Monday through Thursday backups use the same tape with each new backup appended to the previous one. The Friday backup is on a different tape that is archived. The next week you would start all over again with tape 1.

**Note** The number of tapes you need is determined not only by tape rotation, but also by the size of the data that you back up and by the tape life cycle.

The life cycle of a tape depends on the manufacturer and storage conditions. If your company does not have a suitable storage facility, consider using a third-party company that specializes in off-site storage for backup media.

## Backup Sets, Catalogs, and Backup Logs

#### **■ Backup Sets**

 Files and folders from a single volume and a single backup operation

#### **■ Catalogs**

- · Graphical view of the backup
- Automatically created

#### ■ Backup Logs

- Text file record of the backup
- Manually created

Before you do a backup you should know the differences between backup sets, catalogs, and backup logs.

A backup set is term used to describe a group of files or folders on a single volume from a single backup operation. One tape can contain many backup sets.

If a single backup operation requires multiple tapes, the group of tapes is called a family set.

- The *catalog* is a graphical representation of the backup. Windows NT automatically creates catalogs during a backup and stores them on the tape. There are two different catalogs:
  - The tape catalog shows all the backup sets on a tape.
  - The backup set catalog shows all the files and folders in the backup set.

Before you restore files, you must load the catalogs. Then, you can select the backup sets, files, and folders that you want to restore.

■ A backup log is a text file that records backup operations. The backup log is helpful when restoring data, in that you can print it or read it from any text editor. Also, if the tape containing the backup set catalog is corrupt, the printed log will help you locate a file.

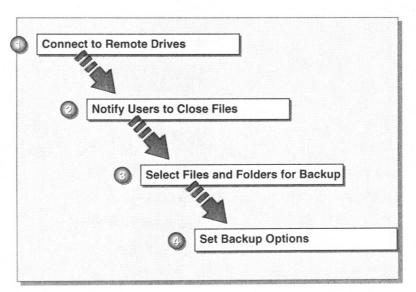
A backup log my contain some or all of the following information, depending on which log options you select:

- Date of backup
- Who performed the backup
- Location of the tape drive

- Tape-set number
- Files backed up
- Type of backup
- Computers backed up

# Backing Up Data

NS. Backup con not Backup a file while it is open.



Performing a backup consists of preliminary tasks as well as tasks in which you use the Windows NT Backup program. The following is an overview of the major tasks:

1. Connect to remote drives.

If you back up remote files, you must first connect to a shared folder on the server where the files are located.

**Note** Windows NT Backup can only back up the Registry or event logs on computers where the tape drive is located.

2. Notify users to close files before you begin the backup. Use **Send Message** in Server Manager.

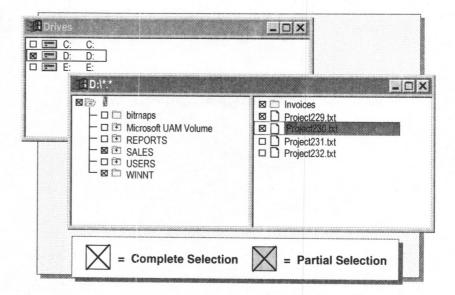
To send a notification, use the following steps:

- a. Start Server Manager.
- b. On the Computer menu, click Send Message.
- c. Type the message to your users, and then click OK.

Windows NT Backup does not back up files locked-open by applications, for example, a Word document currently being edited. The exception is Windows NT operating system files, which can be backed up.

- 3. Start the Windows NT Backup program, and select the files and folders that you want to back up.
- 4. Set the backup options that you want.

## Selecting Drives, Files, and Folders



After you have connected to remote drives and notified users, you can start Windows NT Backup and select the folders and files you want to back up.

### ► To start the Windows NT Backup program

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Backup**. The **Backup** dialog box appears.

**Note** If you want to erase the tape, on the **Operation** menu, click **Erase Tape**.

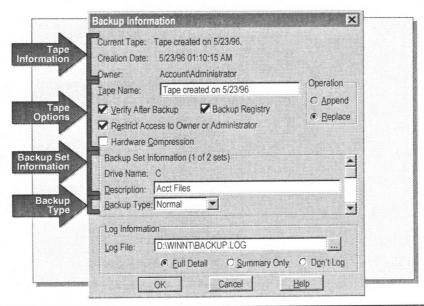
- Maximize the Drives window. The Drives window displays local drives and connected network drives.
- 3. To select all files and folders on a drive, select the check box next to the drive icon.
- 4. To select specific files and folders on a drive, in the Drives window, double-click the drive icon. The *drive\_name* window appears.

This window shows a graphical view of the drive, which is similar to Windows NT Explorer. There are two methods to select files:

- Select the check box next to each folder or file.
- Select the file or folder that you want to back up, and then, on the Select menu, click Check.

**Note** If you do not select all the files and folders on a drive or parent folder, the selected check box appears shaded. This indicates a partial selection.

# **Setting Tape and Backup Options**



After you select the files and folders to back up, set the tape and backup options.

### ► To set tape and backup options

- 1. In the Backup dialog box, click Backup.
  - The **Backup Information** dialog box appears. At the top of the dialog box is tape information, which includes the current tape name, creation date, and the owner of the tape.
- 2. In the **Tape Name** box, type a name that identifies the server being backed up, and where the tape fits into your backup strategy. This name can have up to 32 characters. If you select the **Append** option, the **Tape Name** box is not available.
- 3. Select the following options:

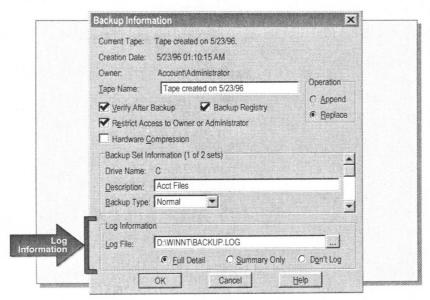
Option	Description
Operation:	Adds a new backup set after the last backup set on the tape.  Overwrites all the data on the tape with the new backup set.
Verify After Backup	Confirms files are backed up accurately.
Backup Registry	Adds a copy of the Registry to the backup set. This option is available only if you select at least one other file on the volume containing the Registry file.
Restrict Access to Owner or Administrator	Limits access to the tape to Administrators, Backup Operators, or the user who performed the backup. If you back up the Registry, you should select this option.
Hardware Compression	Select this option if you use this tape with tape drives that support data compression. This option is available only if the tape drive supports it.

4. In the **Description** box, type in a description of the backup; for example, **Server12 Drive C** 

If there are multiple backup sets, you can type a description for each one. Use the scroll bar at the side of the **Backup Set Information** box to move between backup sets.

- 5. In the **Backup Type** box, click one of the following:
  - Normal
  - Copy
  - Incremental
  - Differential
  - Daily Copy

# **Setting Log Options**



The last section of the **Backup Information** dialog box is the **Log Information** where you can choose to create a backup log.

#### To set up a log

- 1. In the **Log File** box, type the name of the text file used to store the log. The default is Backup.log, and is stored in the \systemroot folder.
- 2. Under Log Information, select one of the following options:

This option	Description
Full Detail	Logs all backup information, including the names of all the files and folders backed up, skipped, and corrupted.
Summary Only	Logs only the major backup operations, such as loading a tape, starting backup, and failing to open a file.
Don't Log	No information is logged.

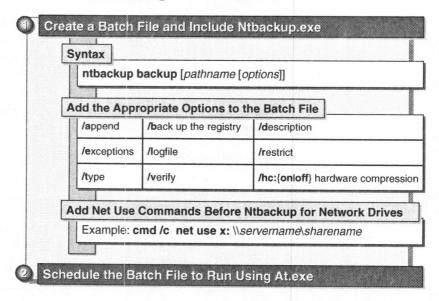
3. Click OK. The Backup Status window appears.

When the backup is finished, you can scroll through the Backup Status window to see if there were any problems on any of the backup sets.

4. Click **OK**. The Drive window appears.

Best Practice Print each backup log. Keep the printed copy in a log book.

# Scheduling a Backup Using a Batch File



You can schedule a batch file backup using the at command (At.exe).

1. Create a batch file that includes the Ntbackup.exe command. Use the following syntax at the command prompt:

ntbackup backup [pathname [options]]

The following table describes options you can use when you create the batch file.

Option	Description
/a	Appends the backup set after any existing backup sets, rather than replacing it. This is not available for a blank tape.
/b	Backs up the local Registry, but only if you back up another file from the same volume.
/d "text"	Describes the backup set. This description appears when you view the tape catalog.
/e	Logs exceptions, such as summary log. If this option is not used, a full detail log is created.
¶ filename	Assigns a file name to the log file. The default is Backup.log in the \systemroot folder.
/r	Limits access to the tape to Administrators, Backup Operators, or the user who performed the backup. If not used, anyone with the restore right can restore the backup set.
/t {Normal   Copy   Incremental   Differential   Daily}	Specifies the backup type. The default backup type is normal.
/v	Confirms that the files were backed up accurately.
/hc: {on   off}	Enables or disables hardware compression for tape drives that support it. The default is hardware compression off.

Continued) Option	Description
cmd /c net use x:	Connects to a remote share. Use this command at the beginning of the command line if you are backing up files on a remote computer—for example:  net use x: \\servername\\sharename. You can also use the UNC name of the shared folder in the backup command.
cmd /c net use x: /delete	Disconnects from a remote share. Use this command at the end of the command line.

2. Use the **at** command (At.exe) to schedule the batch file to run at a specific time.

**Tip** When you are in the Windows NT Backup program, you can access a Help topic called "Using Batch Files to Do Backups" that lists all the command line options and provides examples. To access the topic, press F1 in the Windows NT Backup program to start Backup Help, switch to the **Index** tab, and type **backup**, **using batch files** and then click **Display**.

## **Example of a Scheduled Backup**

#### **Batch File**

cmd /c net use x: \\student1\public
cmd /c net use y: \\student2\public
ntbackup backup c: d: x: y: \\instructorx\public
/T Incremental /b /hc:on /v /l "c:\weekly.log"
cmd /c net use x: /delete
cmd /c net use y: /delete

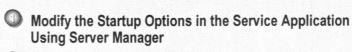
- What Tasks Will This Batch File Perform?
- Which Option Identifies the Tape Content?
- What Command Backs Up Files on a Remote Computer?

#### **Class Discussion**

The slide example shows a batch file with the **ntbackup** command. Review the example to determine the answers to the following questions.

- 1. What tasks will this batch file perform?
- 2. What would you add to this batch file to make it easier to identify the contents of the tape that this batch file creates?
- 3. What command would you add to the batch file to back up files on the remote computer named \Instructorx?

## **Using the At Command**



Use At.exe to Schedule the Task

**Example: At Scheduler** 

At \\student1 00:00 /every: 5,10,15,20,25,30 "backup.bat"

The at command schedules commands to be run by the Schedule service in Windows NT. Because you can use it to schedule commands to run automatically at specified times, you can use the at command to run backup batch files. The Schedule service must be running on the computer that will run the scheduled task.

### ► To start a scheduled backup

■ Use Server Manager to change the Schedule service **Startup Type** to **Automatic**.

This makes the scheduled commands run even if the computer is restarted, regardless of who is logged on.

### ► To modify the startup option in the service application

- Click Start, point to Programs, point to Administrative Tools, and then click Server Manager.
- 2. Under **Computer**, select *computer\_name*, and on the **Computer** menu, click **Services**.

The Services on computer\_name window appears.

3. Under Service, select Schedule, and then click Startup.

The Service on computer\_name window appears.

4. Under **Startup Type**, select **Automatic**, and then click **OK**. The Services on *computer\_name* window appears.

The Schedule service will automatically start the next time the computer is shut down and restarted.

5. Under Service, select Schedule, and then click Start.

The Service Control message window appears with the following message: Attempting to Start the Schedule service on computer\_name.

6. Schedule the tasks using At.exe.

The following is the syntax for the example **at** command, which schedules the backup batch file.

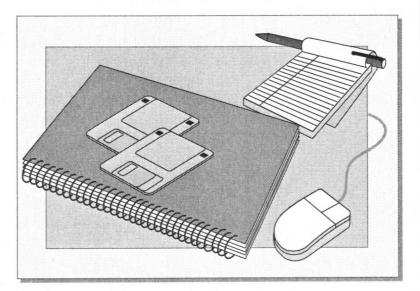
at [\computer\_name] [id] [/delete] time [/interactive][/every: date[,...] | /next: date[,...] "command"

The following table describes the At.exe options.

Option	Description
\\computer_name	Specifies a remote computer. If omitted, the commands are scheduled on the local computer.
id	Assigns an identification number to a scheduled command.
/delete	Cancels a scheduled command. If it is omitted, all the scheduled commands on the computer are canceled.
time	Specifies the time the command is to run. Time is expressed as hour:minutes in 24-hour notation. It runs 00:00 (midnight) though 23:59.
/interactive	Allows the job to interact with the desktop of the user who is logged on at the time the job runs. If omitted, the job will run on an <i>invisible</i> desktop.
/every: date[,]	Specifies the weekdays or days of the month a command is to run. If omitted, the default is the current day of the month.
/next: date[,]	Specifies the next weekdays or days of the month a command is to run. If omitted, the default is the current day of the month.
"command"	Specifies the program or batch file to run, such as Ntbackup.

**Note** The Resource Kit tool Winat.exe is a graphical tool that you can also use to configure tasks for the Schedule service to run.

# Lab 15: Backing Up Data to Tape



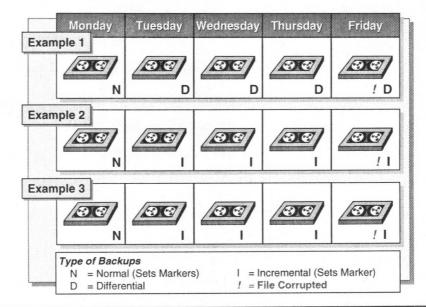
# Implementing a Restore Strategy

- Base Your Restore Strategy on the Backup
- **Keep Documentation for Each Backup**
- **Perform a Trail Restore Periodically**
- Use a Calendar to Record the Backup Frequency and Type

Having a good restore strategy depends on the following:

- A good backup strategy. For example, if you always do a full backup of a volume, in the unlikely event of a disk failure, you can restore the volume in a single operation. Rotating tapes over a period of a week ensures that you can restore an earlier version of a file.
- Keep documentation for each backup. By creating and printing a backup log of each backup, you will be able to quickly locate files that need to be restored without have to load the catalogs from all current backup sets.
  - Depending upon the log you create, the log can include information about the backup type, which files and folders are backed up, and on which tape they are located.
- Perform a trial restore periodically to verify that backed up. A trial restore can uncover hardware problems that do not show up with software verifications.
  - Restore the tape to a drive other than the original drive, and then compare the restored data to the data on the original drive.
- Keep a record of multiple backups in a calendar format showing the days you do backups. By each backup, note the type of backup and a tape identifier, such as a number. Then, if there is a problem, you have a quick glimpse of backups over several weeks and which tape was used for each.

## **Examples of Restore Strategies**



The following are examples of restore strategies. They are based on the backup schedules presented in the graphic above.

### **Example 1: Restoring Normal and Differential Backups**

On Friday an entire volume became corrupted. Based on the backup schedule, restore Monday's normal backup. Then, because the remaining backups are differential, the only additional restore is Thursday's backup.

### Example 2: Restoring Normal and Incremental Backups

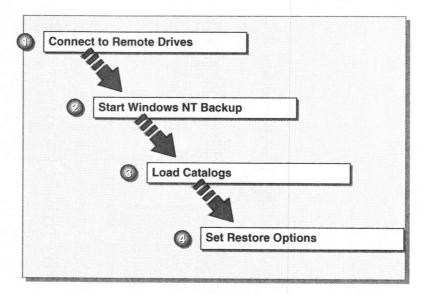
On Friday an entire volume became corrupted. Based on the backup schedule, restore the Monday normal backup. Because the remaining backups are incremental backups, you also need to restore the Tuesday through Thursday backups in that order.

#### **Example 3: Restoring a Single File**

On Friday, one file became corrupted. Because after Monday the backups are incremental backups, you cannot be sure which tape has the most recent copy of the file. Use the backup log to determine when the file was last backed up and which tape contains the backup. Then, restore the file from that tape.

**Important** Make sure the date on your computer is correct. Windows NT Backup uses the date attribute of the file to determine which file version is most current. If you change the date, you may overwrite a file with an older version.

# Restoring Data



When you restore data, you must perform the following tasks.

1. Connect to remote drives.

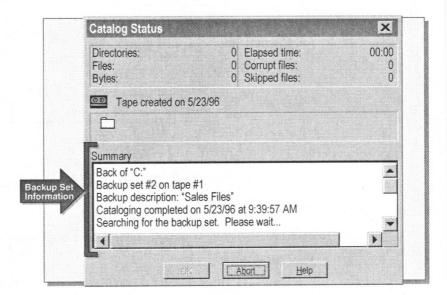
If you restore remote files, you must connect to the appropriate drive on the remote computer before you start the Windows NT Backup program.

**Note** Windows NT Backup can only restore the Registry or event logs on computers where the tape drive is installed.

- 2. Start the Windows NT Backup program.
- Load the tape catalog to view the backup sets.
   Until you load the tape catalog, Windows NT only shows the information for the first backup set.
- 4. Set the restore options that you want.

Your restore procedures will vary slightly depending upon whether you restore a complete tape, backup sets, or individual files and folders.

### Catalogs



You need to load the catalogs to select files and folders. If a backup has multiple tapes, the catalog is on the last tape in the set.

#### ► To load a tape catalog

- 1. Start the Windows NT Backup program and maximize the *tape\_name* window.
- 2. On the **Operation** menu, click **Catalog**. The **Catalog Status** dialog box appears.
- 3. When the catalog finishes loading, click **OK**. The *tape\_name* window maximizes.

On the folder icon of a backup set is a question mark (?). This indicates that the catalog for the backup set is not loaded.

#### ► To load a backup set catalog

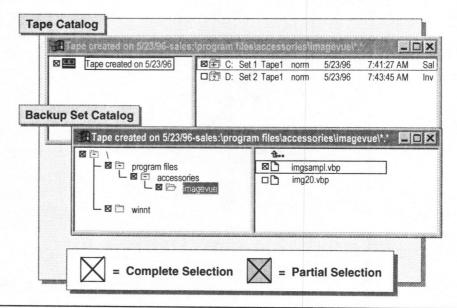
- 1. In the *tape\_name* window, double-click the appropriate backup set folder. The **Catalog Status** dialog box appears.
- 2. When the catalog finishes loading, click **OK**. The *tape\_name* window appears with the folder tree for the backup set.

Once the catalog for a backup set is loaded, the question mark (?) on the folder changes to a plus sign (+). To see this, maximize the *tape\_name* window.

If there are corrupted files on the tape, the files' corresponding folders are marked with a red X.

**Important** If the last tape in a family set is missing or damaged, you can force Windows NT Backup to treat the data on each remaining tape as a single unit, by starting Windows NT Backup from the command prompt with the **/missingtape** option.

## Selecting Backup Sets, Files, and Folders



Once you have loaded the tape catalog, you can select backup sets or specific files and folders to restore.

### ► To select a backup set

■ In the *tape\_name* window, select the check boxes of the backup set or sets that you want to restore.

-or-

Select a backup set, and then on the **Select** menu, click **Check**. Repeat this step for the remaining backup sets that you want to restore.

### ► To select individual files and folders in a backup set

- 1. If you need to expand a subfolder in the *backup\_set* window, double-click the appropriate folder.
- 2. In the expanded folder tree of the *backup\_set* window, use either of the following methods:
  - Select the check boxes next to files or folders you want to restore.

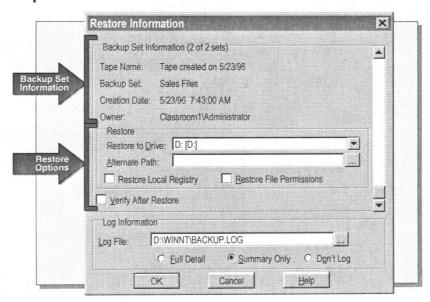
-or-

• Select the file or folder you want to restore. Then on the **Select** menu, click **Check**.

An X appears in the check box of the file or folder that you select, and in the boxes of the parent folder and disk drive. If you select only some of the folders and files of a disk drive or parent folder, the check box appears shaded.

**Note** You can select multiple files and folders by pressing the SHIFT key or the CTRL key and clicking the files or folders.

## **Selecting Restore Options**



After you have selected the files and folders to backup, select the restore options that you want.

### **▶** To select restore options

1. In the **Backup** dialog box, click **Restore**. The **Restore Information** dialog box appears.

Under **Backup Set Information**, you will find information about the number of backup sets, tape name, backup set description, tape creation date, and tape owner.

2. In the **Restore to Drive** box, click the drive to restore to. The default drive is the original drive.

You can select a different drive than the source drive for each backup set you are restoring.

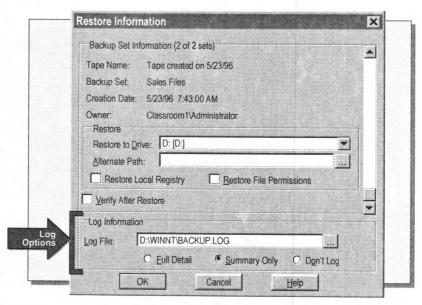
3. If you want to restore a backup set into a different location than the original one, type an alternate directory path. You can browse to select this path.

**Tip** To verify backup and restore are operating correctly, restore the tape to a different drive. Then compare the original file and the restored file.

4. Select any of the following restore options.

Option	Description
Restore Local Registry	Restores the Registry file. For the changes to the Registry files to take effect, shut down and restart the computer.
Restore File Permissions	Restores the NTFS permissions. If not selected, files inherit the permissions of the folder to which they are restored.
	Do not restore file permissions if you restore to a computer that does not have the same user and group accounts.
Verify After Restore	Verifies the content of the files restored to disk against the files on the tape. Windows NT Backup logs exceptions.

# **Selecting Log Options**



After you select the restore options, then select the log options you want.

### **▶** To select log options

1. Select any of the following log options.

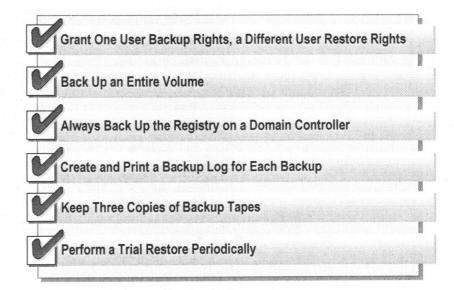
Option	Description
Log File	The location of the text file for logging all tape operations. You can browse to find the correct name.
Log Information	
• Full Detail	Logs all information on all restore operations including the names of all files and folders restored.
• Summary Only	Logs only the major operations, such as loading a tape, starting restore, and failing to restore a file.
• Don't Log	Logs nothing.

2. Click **OK**. The Restore Status window appears with a description of the restore process, and then it changes to the Verify Status window.

**Note** During this process the **Confirm File Replacement** dialog box appears. Click either **Yes** to overwrite one file at a time, or **Yes To All** to overwrite all existing files without being prompted again.

3. When the restore process finishes, the message "The operation was successfully completed" appears. Click **OK**. The **Backup** dialog box appears. The restore process is finished.

## **Best Practices**



The following list provides best practices for backing up and restoring data:

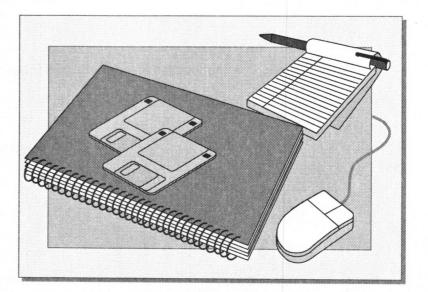
- In minimum and medium security networks, grant one user backup rights and a different user restore rights.
  - You should grant only backup rights by removing the *Restore Files and Directories* user right from the Backup Operators and Server Operators groups.
  - You should grant only restore rights by creating a local group named Restore Operators and then assigning the *Restore Directories and Files* user right to the group. Then, create a global group named Restore Only and add it to the local group.

Note In a high security network, only administrators should restore data.

- Back up an entire volume in the unlikely event of a disk failure. It is more
  efficient to restore the entire volume in one operation.
- Always back up the Registry on a domain controller to prevent the loss of user account and security information.
- Always create and print a backup log for each backup. Keep a book of logs to make it easier to locate specific files.
- Keep three copies of tapes. Keep at least one copy off-site in a properly controlled environment.
- Perform a trial restore periodically to verify that your files were properly backed up. A trial restore can uncover hardware problems that do not show up with software verifications.

**Note** Secure both the tape drive and the backup tapes. Someone can access the data from a stolen tape by restoring the data to another server for which they are an administrator.

# **Lab 16: Restoring Data from Tape**



# **Review**

- Introduction to the Windows NT Backup Program
- Planning a Backup Strategy
- Backing Up Data
- Scheduling a Backup Using a Batch File
- Implementing a Restore Strategy
- Restoring Data
- **Best Practices**
- 1. Which files should you always back up?
- 2. How do backup markers affect backups?
- 3. What methods can you use to control who can restore a backup tape?
- 4. What three steps should you take to ensure that your backups and restores are complete and accurate?

- 5. You need to restore a particular file. You did a normal backup yesterday, but you forgot to create a backup log. How do you find the file?
- 6. You need to restore the server data. The backup for the data consists of multiple tapes of which the last tape is damaged. What can you do?