

Microsoft® Windows® Server 2003 Deployment Kit

Designing a Managed Environment

A Resource Kit Publication

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. 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.

© 2003 Microsoft Corporation. All rights reserved.

Active Directory, ActiveX, FrontPage, JScript, Microsoft, Microsoft Press, MS, MSDN, MS-DOS, Notepad, SQL Server, Visual Basic, Visual Studio, Windows, Windows Media, Windows NT, and Win32 are registered trademarks of Microsoft Corporation in the USA and other countries.

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

IBM is a registered trademark of International Business Machines Corporation.

NetWare is a registered trademark of the Novell Corporation.

Apple and Macintosh are registered trademarks of the Apple Corporation.

ActivePerl is a registered trademark of the ActiveState Corporation.

Contents at a glance

INTRODUCTION	xvii
CHAPTER 1 Planning a Managed Environment	1
CHAPTER 2 Designing a Group Policy Infrastructure	51
CHAPTER 3 Staging Group Policy Deployments	119
CHAPTER 4 Deploying Security Policy	157
CHAPTER 5 Deploying Microsoft Software Update Services	197
CHAPTER 6 Migrating User State	235
CHAPTER 7 Implementing User State Management	263
CHAPTER 8 Deploying a Managed Software Environment	343
CHAPTER 9 Deploying a Simple Managed Environment	429
GLOSSARY	481
INDEX.....	495

Contents

INTRODUCTION	xvii
Deployment Kit Compact Disc	xviii
Document Conventions	xix
Support Policy	xxiii
CHAPTER 1 Planning a Managed Environment	1
Overview of Deploying a Managed Environment Process	2
IntelliMirror Deployment Process	4
Introduction to IntelliMirror Configuration Management Technologies	7
IntelliMirror Technologies	8
IntelliMirror Implementation Examples	11
Setting up the New Employee's Computer Example	12
Logging on the First Time Example	12
Making Offline Files Accessible to a Portable Computer Example	13
Setting up a Shared Computer Environment Example	13
Replacing a Computer Example	14
Implementing a Customized Home Page URL for all Domain Users Example	14
Managing Desktops in Non-Active Directory Environments	15
Developing a Deployment Plan	16
Defining the Scope of Your Configuration Management Project	17
Assessing Your Current Environment	18
Evaluating Your Desktop Management Processes	19
Evaluating Computer and User Roles	20
Categorizing Users by Job Types and Location	20
Evaluating Your Security Requirements	23
Determining Corporate Policies	24

vi Contents

Assessing Network and Storage Requirements	24
Determining Your Requirements for Configuration Management Technologies	28
Identifying the IntelliMirror Technologies That Meet Your Configuration Management Needs	31
Designing Managed Configurations	37
Mapping Managed Configurations to User and Computer Roles	37
Designing Your Organizational Unit Structure	44
Application of Group Policy	45
Testing Your Configuration Management Design	45
Conducting Proof of Concept Testing	46
Conducting Pilot Testing	47
Preparing Users for Deployment	47
Staging and Deploying Your Design to the Production Environment	48
Additional Resources	48
CHAPTER 2 Designing a Group Policy Infrastructure	51
Group Policy Overview	52
Process for Implementing a Group Policy Solution	54
What You Need Before Designing Your Group Policy Solution	55
New in Windows Server 2003: Group Policy Management	56
Planning Your Group Policy Design	58
Designing an OU Structure that Supports Group Policy	59
Complying with Service Level Agreements	62
Defining Your Group Policy Objectives	63
Establishing Group Policy Operational Guidelines	64
Identifying Interoperability Issues	65
Determining When Group Policy Changes are Applied	66
Identifying Issues Pertaining to Software Installation	68
Designing Your Group Policy Model	68
Defining the Scope of Application of Group Policy	70
Determining the Number of Group Policy Objects	72
Linking GPOs	73
Using Security Filtering to Apply GPOs to Selected Groups	75
Applying WMI Filters	76
Using Group Policy Inheritance	80
Deploying Group Policy	82
Creating and Working with GPOs	83

Using Loopback Processing to Configure User Settings	87
Delegating Administration of Group Policy	88
Defining Group Policy Operational Procedures	93
Specifying a Domain Controller for Editing Group Policy	94
Group Policy and Slow Links	95
Specifying Group Policy for Slow Link Detection	96
Controlling Client-Side Extensions by Using Group Policy	99
Minimizing the Growth of DC System Volume Folders	
Changing the Group Policy Refresh Interval	103
Using Group Policy Modeling and Group Policy Results to Evaluate Group Policy Settings	105
Backing up, Restoring, Migrating, and Copying GPOs	108
Maintaining Group Policy	115
Group Policy Considerations for Renaming a Domain	116
Using Scripts to Manage Group Policy	117
Additional Resources	117
CHAPTER 3 Staging Group Policy Deployments	119
Overview of Group Policy Staging	120
Group Policy Staging Process	121
GPMC Staging Technology Background	122
Creating the Staging Environment	126
Synchronizing the Staging and Production Environments	130
Example: Creating an XML Format File from a Production Environment	132
Importing Production GPOs into the Staging Domain	133
Example: Populating the Staging Domain from the XML Format File	134
Maintaining Synchronization of Staging and Production	135
Testing Group Policy in the Staging Environment	136
Preparing for Deployment to Production	140
Creating Migration Tables	141
Deploying Staged GPOs to the Production Environment	148
Deployment Precautions	149
Deployment Examples	150
Additional Resources	156
CHAPTER 4 Deploying Security Policy	157
Overview of Security Policy Deployment	158
Security Policy Deployment Process	159
Security Policy Concepts	160

viii Contents

Group Policy Management Console	160
Security Configuration Manager	161
Designing Security Policy	162
Designing IPSec Policies	163
Designing Security Settings	167
Using Custom Security Templates	169
Selecting Predefined Security Templates	169
Design Recommendations for Using Predefined Security Templates	175
Refreshing Group Policy to Activate New Settings	176
Designing Software Restriction Policies	
Designing Wireless Network Policies	177
Design Considerations for Wireless Network Policies	178
Understanding Wireless Network Policy Precedence	179
Measuring Your Design Using the GPMC	180
Configuring Security Policy	181
Configuring Security Settings for Sites, Domains, and OUs	182
Importing Security Templates and Modifying Security Settings in a GPO	182
Modifying Account Policies in the Default Domain GPO	183
Modifying Local Policies in the Default Domain Controllers GPO	185
Implementing Software Restriction Policies	186
Configuring Wireless Network Policies	189
Creating Wireless Network Policies	192
Defining Wireless Configuration Options for Preferred Networks	192
Testing Security Policies and Rolling Out a Pilot Project	194
Additional Resources	194
CHAPTER 5 Deploying Microsoft Software Update Services	197
Software Update Services Overview	198
Implementing a SUS Solution	198
Technology Background	199
Distinguishing Patch Designations	199
Server Component	201
SUS Client Component	202
SUS Security Features	204
Designing the Server Deployment	205
Determining Your Internet Connectivity	206

Scaling Out Your SUS Server Deployment	207
Multiple Internally Synchronized Servers Running SUS	209
Multiple Servers Running SUS and NLB	210
Deploying the SUS Server Component	211
Installing the SUS Server Software	212
Configuring the SUS Server	212
Running SUS with IIS	216
Creating Distribution Points	218
Securing SUS Administration	219
Configuring SUS for Use with NLB	220
Synchronizing Content	221
Synchronizing the List of Approved Packages	222
Approving Updates	222
Reviewing Server Actions and Server Functionality	223
Staging Content	225
Deploying Automatic Updates	226
Centrally Deploying Automatic Updates	227
Configuring Automatic Updates	229
Administrative Methods for Configuring Automatic Updates	230
Additional Resources	233
CHAPTER 6 Migrating User State	235
Overview of Migrating User State	236
User State Migration Process	237
Tools Used in the Migration Process	238
Choosing a User State Collection Method	241
Manual Migration	243
Scripted-Manual Migration	244
Centralized Automation	245
User-Driven Migration	247
Identifying Migration Content	248
Identifying User Data to Migrate	248
Identifying User Settings to Migrate	249
Identifying Key Settings for User Productivity	249
Evaluating Costs vs. Benefits of Migrating Settings	250
Creating a Detailed Migration Plan	251
Resolving Storage and Data Issues	252
Determining Storage Requirements	252

x Contents

Reviewing Data Collection and Restoration Selections	253
Addressing File Relocation Issues	253
Identifying Security Concerns	253
Restoring Lost Access Control Lists (ACLs)	254
Managing Data Encryption During Migration	254
Securing User State During Migration	255
Translating and Relocating Registry Entries	255
Adapting Your Plan for Domain Migration	256
Scheduling Your Migration	257
Educating Users	257
Testing Your Migration Process	258
Performing Lab Tests	259
Performing a Pilot Test	259
Additional Resources	260
CHAPTER 7 Implementing User State Management	263
Implementing User State Management Overview	264
User State Management Implementation Process	265
Technology Background	266
Planning for User State Management	273
Determining User Requirements	274
Evaluating Computer Services	274
Determining Storage Requirements for Users, Local Workstation, and Servers	275
Assessing Network Bandwidth Availability and Requirements	277
Designing Configurations for Managed Desktops	278
Creating a New User Desktop Configuration	280
Designing Managed Configurations for Mobile Users	281
Recommendations for Configuring Mobile Users Computers	284
Designing Highly Managed Desktops	285
Designing Lightly Managed Desktops	286
Designing Managed Multi-User Desktops	286
Designing Managed Desktops for Replacing Computers	288
Preparing for Deployment	289
Performing Controlled Testing	290
Piloting a Limited Deployment	290
Preparing Users	290
Teaching Users about Roaming Profiles	290

Teaching Users about Folder Redirection	291
Teaching Users about Offline Files and Synchronization Manager	291
Teaching Users about Disk and Profile Quotas	292
Configuring User State Management Features	293
Implementing Roaming User Profiles	295
Recommendations for Roaming User Profiles	295
Group Policy Recommendations for Roaming User Profiles	296
Security Recommendations for Roaming User Profiles Shared Folders	300
Configuring Roaming User Profiles	303
Implementing Folder Redirection	307
Recommendations for Folder Redirection	308
Group Policy Recommendations for Folder Redirection	312
Security Recommendations for Folder Redirection	314
Configuring Folder Redirection	316
Implementing Offline Files and Synchronization	320
Recommendations for Using Offline Files	320
Configuring Group Policy for Offline Files	324
Security Recommendations for Shared Resources	329
Configuring Offline Files	331
Configuring Synchronization Manager	333
Assigning Profile and Disk Quotas	334
Setting Quotas on User Profiles	335
Over-Allocating Disk Space	336
Configuring Disk Quotas on NTFS Volumes	338
Desktop Strategies for Computers Running Windows 2000 and Windows XP Without Active Directory	340
Additional Resources	341
CHAPTER 8 Deploying a Managed Software Environment	343
Deploying a Managed Software Environment Overview	344
Deploying a Managed Software Environment Process	345
Assessing Microsoft Software Management Solutions	346
Group Policy Software Deployment Background	349
Preparing Applications for Deployment	352
Determining the Preparation Method	354
Packaging Software for Deployment	357
Deploying Applications in a Managed Environment	370

Determining Requirements for Software Distribution Point Servers	377
Configuring Software Distribution Point Servers	378
Targeting Software to Users and Computers	381
Assigning and Publishing Software	387
Categorizing Applications	392
Conducting a Pilot for Software Deployment	393
Making Software Available to Users and Computers	398
Migrating Applications to a Managed Environment	400
Patching, Upgrading, and Removing Applications	405
Patching Installed Applications	407
Upgrading Installed Applications	408
Removing Installed Applications	412
Restricting Software Access and Protecting Computers	413
Patching, Upgrading, and Removing Software Examples	418
Troubleshooting Software Deployment	420
Using GPMC Group Policy Modeling to Evaluate Group Policy Settings Before Deployment	422
Using GPMC Group Policy Results to Evaluate Group Policy Settings After Deployment	423
Additional Resources	426
CHAPTER 9 Deploying a Simple Managed Environment	429
Overview of Deploying a Simple Managed Environment	430
Process for Deploying a Simple Managed Environment	431
Chapter Assumptions and Sample Configuration	432
Deploying the Network Infrastructure	435
Setting Up the Physical Network	436
Deploying a Domain Controller Inside the Intranet	437
Install and Configure the Domain Controller	437
Synchronize the Time Server for the Domain Controller with an External Source	442
Format Additional Drive Partitions	443
Deploying Windows XP Professional	444
Deploying the Logical Infrastructure	447
Installing Group Policy Management Console (GPMC)	448
Creating a Basic OU Structure	448
Deploying Security Policies	451
Preparing Shared Folders	452

Creating a DFS Root Share	453
Creating Server Shares for Applications	455
Creating Server Shares for User Data	456
Installing Software	458
Installing MS Office and the Administrative Tools Package	459
Installing Software Update Services	460
Setting Policies to Manage User Data and Settings	462
Setting Policies for All Users	463
Setting Policies for Users with Roaming User Profiles	467
Setting Policies for the Users in the IT OU to Access the Administrative Tools Pack	469
Setting Policies for Mobile Users	470
Testing and Deploying Your Configuration	470
Linking GPOs and Using Group Policy Modeling to View the Results	472
Testing Computers and Users	474
Backing Up the Server	476
Deploying Your Configuration	478
Additional Resources	478
GLOSSARY	481
INDEX	495

Acknowledgments

Microsoft would like to thank the following people for their contributions:

Book Leads: Chris McKitterick, Kelly Vomacka

Lead Technical Writer: Deborah R. Jay

Writers: John Kaiser, Darren Mar-Elia, Merrilee McDonald, Michael McGinnis, Chris McKitterick, Joy Miller, Patricia Nicholson, Dionysia Sofos

Book Editor: Paula Younkin

Editors: Nona Allison, Ann Becherer, Jim Becker, Bonnie Birger, Dale Callison, Sandra Faucett, Julie Geren, Anika Nelson, Tyler Parris, Monica Sharp, Fredrika Sprengle, Dee Teodoro, Scott Turnbull, Scot Yonan, Julia Ziobro

Documentation Manager: Pilar Ackerman

Writing Lead: Cheryl Jenkins

Editing Leads: Laura Graham, Kate O’Leary, Scott Somohano

Lab Management: Robert Thingwold, David Meyer

Project Managers: Clifton Hall, Paulette McKay, Neil Orint

Online Components Writing Team: Peter Costantini, Eve Gordon, Amy Groncznack, Lola Gunter, Sean Loosier, Irfan Mirza, Gary Moore, Chris Revelle, Kim Simmons, Greg Stemp, Dean Tsaltas, Kelly Vomacka

Online Components Editing Team: Anika Nelson, Kate Robinson, Dee Teodoro

Windows Server Resource Kit Tools Program Managers: Majdi Badarin, Clark Gilder

Resource Kit Tools Software Development and Test Team: Sameer Garde, Sunil Gummalla, Venu Somineni, Kendra Yourtee, Scott Smith, John Turner

Publishing Team: Barbara Arend, Jon Billow, Chris Blanton, Eric Camplin, Yong Ok Chung, Andrea DeGrazia, Julie Geren, Jason Hershey, Michael Howe, Richard Min, Cornel Moiceanu, Rochelle Parry, Mark Pengra, Steve Pyron, Ben Rangel, Gino Segal, Amy Shear, Karla van der Hoeven, Gabriel Varela, Ken Western, Matt Winberry

Indexing Team: Julie Hatley, David Pearlstein

Key Technical Reviewers: Linda Apsley, Paul Darcy, Michael Dennis, Judith Herman, Craig Marl, BJ Whalen, Mark Williams

Technical Reviewers: Bill Anderson, Arun Ayyagari, Ritu Bahl, Drew Baron, Ara Bernardi, Stephan Betz, Duncan Bryce, John Case, Bruce Clayton, Arren Conner, Nathan Cornillon, Don Cottam, Joseph Dadzie, David Dehghan, William Dixon, Tina Duff, Mercy Dworzak, Greg Feiges, Brian Granowitz, Brent Hatfield, Ian Hellen, Gary Henderson, Atul Patel Hirpara, Jin Huang, Krishnan P. Iyer, Anton Krantz, Stuart Kwan, John Lambert, Paul LeBlanc, Elliot Lewis, Ian Lindsay, Steve Lipner, Andreas Luther, Chris Macaulay, Taroon Mandhana, Jim Masson, Gary Moore, Arun Nanda, Calin Negreanu, Frank Olivier, Adam Overton, Anshul Rawat, Tony Reveal, David Rheaume, Jason Rush, Mohammed Samji, Dave Sayers, Brad Shantz, Wallace Simpson, Raymond Sinnappan, Judi Smith, Kirk Soluk, Lara Sosnosky, David Steere, Florin Teodorescu, Tim Thompson, Melissa Torry, Mike Treit, Mike Truitt, Steve Whitford, Helga Widmann, Yi Zhao, Jill Zoeller

Special thanks to Martin DelRe for his support and sponsorship. Without his contribution, the publication of this kit would not have been possible.

Introduction

Welcome to *Deploying a Managed Environment* of the *Microsoft® Windows® Server 2003 Deployment Kit*.

This book provides the foundation you need to understand and deploy Group Policy and its supporting technologies, included within Microsoft® Windows® Server 2003. The guidance in this book will help you reduce the cost of managing a diverse set of organizational and computing needs, and to centrally manage domain-wide and forest-wide security, servers, computers, and users.

Deployment Kit Compact Disc

The following contents are included on the *Windows Server 2003 Deployment Kit* companion CD:













- **Windows Server 2003 Deployment Kit.** A searchable online version of the *Windows Server 2003 Deployment Kit*.
- **Resource Kit Tools for Windows Server 2003.** A collection of tools included with the Windows Deployment and Resource Kits that can help you deploy, configure, maintain, and troubleshoot Windows Server 2003.
- **Resource Kit Registry Reference for Windows Server 2003.** A searchable online reference providing detailed descriptions of the Windows Server 2003 registry, including many entries that cannot be edited by using Windows Server 2003 tools or programming interfaces.
- **Resource Kit Performance Counters Reference for Windows Server 2003.** A searchable online reference describing what each performance counter monitors. You can use performance counters to diagnose problems or detect bottlenecks in your system.
- **Deploying Internet Information Services (IIS) 6.0 & Migration Tools.** A searchable online version of *Deploying Internet Information Services (IIS) 6.0* and tools that you can use to migrate to IIS 6.0.
- **Job Aids for the Windows Server 2003 Deployment Kit.** Worksheets and resources that can help you create your deployment plan for Windows Server 2003.
- **Windows Server 2003 Help.** The searchable Help file included with the Windows Server 2003 operating system containing technical content for the IT professional, which can be installed on Microsoft® Windows® XP Professional.
- **Microsoft Office Viewers.** Viewers you can install on your computer if you do not have Microsoft® Office, which allow you to see worksheets and resources on the *Windows Server 2003 Deployment Kit* companion CD.
- **CD-ROM Release Notes.** Late breaking information about the contents of the *Windows Server 2003 Deployment Kit* companion CD.
- **Links to Microsoft Press.** Links to the Microsoft Press Support site, which you can search for Knowledge Base articles, and to the Microsoft Press product registration site, which you can use to register this book online.

Document Conventions

The following art symbols and text conventions are used throughout this book.









Flowchart Symbols

Use the following table of symbols as a resource for understanding the flowcharts included in this guide.

Symbol	Meaning	Symbol	Meaning
	Step or component process		Data stored to a database
	Predefined process or subroutine		Flowchart beginning or end
	Decision point		Intra-chart connector: Flow continues to next page
	Output to a document or input from a document		Intra-chart connector: Flow continues from previous page
	Data transfer to a file on disk		Inter-chart connector: Indicates an exit point to another flowchart
	Data transfer to a data store		Inter-chart connector: Indicates an entry point from another flowchart



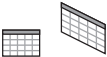
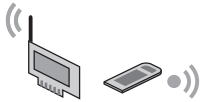





















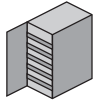
Art Symbols

Use the following table of the art symbols as a resource for understanding the graphics included in this guide.

Symbol	Meaning	Symbol	Meaning
	Workstation		Macintosh client
	Portable computer		Tablet computer
	Terminal		Cellular phone
	Portable digital assistant (PDA)		Document



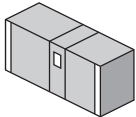
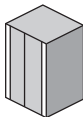





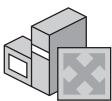

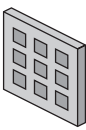
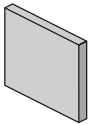
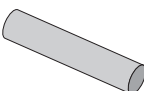






(continued)

(continued)

Symbol	Meaning	Symbol	Meaning
	File folder		E-mail
	Chart		Wireless network adapter
	Modem		Video camera
	Network adapter		Digital camera
	Facsimile		Printer
	Telephone		Scanner
	Hard disk		Tape drive
	Database		Tape
	Compact disc		Security key
	Digital certificate		Padlock
	Padlock		Uninterruptible power supply
	Access token		Hub
	Modem bank		Automated library











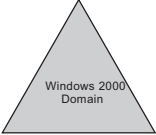
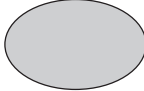
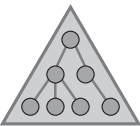
(continued)

(continued)

Symbol	Meaning	Symbol	Meaning
	Windows NT-based server		Generic server
	Mainframe computer		Host
	Server farm		Clustered servers
	Router		Switch
	Shadowed router		Windows 2000-based router
	Data jack		Input/output (I/O) filter
	Firewall		Tunnel
	Internet		An intranet
	Transceiver		Script
	Interface		Packets






(continued)

(continued)

Symbol	Meaning	Symbol	Meaning
	Process or communication failure		DNS root
	Directory tree root		Root
	Organization		Organizational unit
	Common name		Generic node
	Active Directory domain		User group
	Windows 2000 domain		Site or Windows NT 4.0 domain
	Active Directory™		

Reader Alert Conventions

Reader alerts are used throughout this guide to notify you of both supplementary and essential information. The following table explains the meaning of each alert.

Reader Alert	Meaning
 Tip	Alerts you to supplementary information that is not essential to the completion of the task at hand.
 Note	Alerts you to supplementary information.
 Important	Alerts you to supplementary information that is essential to the completion of a task.
 Caution	Alerts you to possible data loss, breaches of security, or other more serious problems.
 Warning	Alerts you that failure to take or avoid a specific action might result in physical harm to you or to the hardware.

Command-line Style Conventions

The following style conventions are used in documenting scripting and command-line tasks throughout this book.

Element	Meaning
bold font	Characters that you type exactly as shown, including commands and parameters. User interface elements are also bold.
<i>Italic font</i>	Variables for which you supply a specific value. For example, <i>Filename.ext</i> can refer to any valid file name.
Monospace font	Code samples.
Command	Command that is typed at the command prompt.
Syntax	Syntax of script elements.
Output	Output from running a script.

Support Policy

Microsoft does not support the software supplied in the *Windows Server 2003 Deployment Kit*. Microsoft does not guarantee the performance of the scripting examples, job aids, or tools, bug fixes for the tools, or response times for answering questions. However, we do provide a way for customers who purchase the *Windows Server 2003 Deployment Kit* to report any problems with the software and receive feedback for such issues. You can do this by sending e-mail to rkinput@microsoft.com. This e-mail address is only for issues related to the *Windows Server 2003 Deployment Kit*. For issues related to the Windows Server 2003 operating systems, please refer to the support information included with your product.

Planning a Managed Environment

1

Many organizations are moving towards a highly managed computing environment based on a configuration management infrastructure that is designed to reduce the cost of managing a diverse set of organizational needs. The Microsoft® Windows® Server 2003 operating system includes a set of configuration management technologies — collectively known as IntelliMirror® — that you can use to centrally manage configurations for users and computers.

IntelliMirror and Group Policy combine the advantages of centralized computing with the performance and flexibility of distributed computing. This book explains how to design and deploy a centrally managed distributed computing environment.

In This Chapter

Overview of Deploying a Managed Environment Process	2
Developing a Deployment Plan	16
Defining the Scope of Your Configuration Management Project	17
Assessing Your Current Environment	18
Determining Your Requirements for Configuration Management Technologies	28
Designing Managed Configurations	37
Designing Your Organizational Unit Structure	44
Testing Your Configuration Management Design	45
Staging and Deploying Your Design to the Production Environment	48
Additional Resources	48

Related Information

- For more information about designing and deploying your Active Directory® directory service infrastructure, see “Planning an Active Directory Deployment Project” and “Designing the Active Directory Logical Structure” in *Designing and Deploying Directory and Security Services* of this kit.
- For more information about Group Policy, see the *Distributed Services Guide* of the *Microsoft® Windows® Server 2003 Resource Kit* (or see the *Distributed Services Guide* on the Web at <http://www.microsoft.com/reskit>).

Overview of Deploying a Managed Environment Process

The IntelliMirror technologies included in Microsoft® Windows® 2000, Microsoft® Windows® XP, and Windows Server 2003 operating systems provide the capabilities for directory-based configuration management. By using IntelliMirror on the server and the client, you can ensure that a user's data, applications, and settings remain constant throughout the user's environment. You also use Group Policy to centralize the process for deploying and managing security for servers running Windows 2000 and Windows Server 2003 and clients running Windows 2000 and Microsoft® Windows® XP Professional. Together, Active Directory and Group Policy provide the foundation for IntelliMirror. Based on the Group Policy settings you specify, IntelliMirror can deploy, recover, restore, and replace user's data, software, and personal settings. You can set policy definitions once and rely on the system to apply the policy settings without further administrative intervention. By using IntelliMirror, you can centralize and simplify the management of users, servers, desktops, and security.

The term *configuration management* as used in this guide refers to a subset of technologies in Windows Server 2003 (and Windows 2000) that administrators can use as part of their overall infrastructure for change and configuration management. By using the IntelliMirror management technologies provided in Windows 2000 and later, you can design configurations for servers, desktops, and users.

Microsoft has developed guidelines you can use to help you effectively design, develop, deploy, operate, and support solutions built on Microsoft technologies. The guidelines are organized into two integrated frameworks, Microsoft Operations Framework (MOF) and Microsoft Solutions Framework (MSF). The guidelines include white papers, operations guides, assessment tools, best practices, case studies, templates, support tools, and services. MOF provides technical guidance that enables organizations to achieve system reliability, availability, supportability, and manageability of IT solutions. MOF addresses the people, process, technology, and management issues pertaining to operating complex, distributed, heterogeneous IT environments.

For more information about MOF, see the Microsoft Operations Framework (MOF) link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>. For more information about Microsoft Solutions Framework, see the Microsoft Solutions Framework link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Advantages of Using IntelliMirror

IntelliMirror refers to the ability to provide users with consistent access to their applications, application settings, roaming user profiles, and user data, from any managed computer – even when they are disconnected from the network. IntelliMirror is delivered via a set of Windows features that enable IT administrators to implement standard computing environments for groups of users and computers.

IntelliMirror can significantly boost user productivity and satisfaction by doing the following:

- Allowing users to continue working efficiently in intermittently connected or disconnected scenarios by enabling uninterrupted access to user and configuration data under these conditions.
- Delivering a consistent computing environment to users from any computer when their desktop or laptop computer is unavailable or in scenarios where users are not assigned a specific computer.
- Minimizing data loss by enabling centralized backup of user data and configuration files by the IT organization.
- Minimizing user downtime by enabling automated installation and repair of applications.

Implementing IntelliMirror also boosts administrator efficiency and reduces IT costs by doing the following:

- Eliminating the need to manually configure user settings, install applications, or transfer user files to provide users access to their computing environments on any computer.
- Enabling scenarios where users don't have an assigned computer but log on to any available computer in a pool of computers. This helps reduce hardware and administration costs.
- Easing the IT task of implementing centralized backup of user files while satisfying need for these files to be available on the user's computer.
- Reducing support costs by using Windows Installer to automatically repair broken application installations.

IntelliMirror is implemented by means of a set of Windows features, including Active Directory, Group Policy, Software Installation, Windows Installer, Folder Redirection, Offline Folders, and Roaming User Profiles.

Deploying IntelliMirror technologies for configuration management provides the following advantages.

User data management IntelliMirror facilitates the centralized backup and restore of user data. Storing the users data on servers simplifies data backup and security and ensures that data is protected and highly available. Users can access their data from any computer on the network. *User data management* relies on Active Directory, Group Policy, Folder Redirection, Offline Files, and disk quotas.

User settings management Using the *user settings management* capabilities, you can manage user settings and preferences (such as user-defined screen colors and display fonts) and make them available to users regardless of which networked computer the users log on to. You can centrally define managed configurations for users and mirror user settings to the network. *User settings management* relies on Active Directory, Group Policy, Roaming User Profiles, Folder Redirection, Offline Files, and Synchronization Manager.

Security settings Using Group Policy, you can manage the following types of *security* options for users, clients, servers, and domain controllers: Internet Protocol security (IPSec), security settings, software restrictions policies, and wireless network policies.

Group Policy–based software installation Using *Group Policy–based software installation*, you can manage software installation throughout an application’s life cycle. You can centrally manage software installation, repairs, updates, and removal.

Internet Explorer policy settings Using *Microsoft® Internet Explorer policy settings* you can customize the appearance of the browser, define connection settings, and define custom Universal Resource Locators (URLs), security settings, and program associations.

Scripts You can specify scripts to run when the computer starts and shuts down and when users log on or log off.

Remote setup and configuration Using *Remote Installation Services (RIS)*, you can simplify operating system installations by remotely setting up and configuring operating system installations on computers throughout the enterprise.

To ensure the success of your managed environment deployment, you must create a configuration management plan that defines the resources to be managed and the processes that you are implementing.

You start your deployment plan by defining your business objectives for change and configuration management and determining the scope of your configuration management deployment in terms of the users and resources you need to manage. In the first phase, you also need to perform an assessment of your current environment and determine the requirements for configuration management.

Next, determine which IntelliMirror configuration management technologies meet your business requirements, and then design managed configurations for the various types of users and computers in your organization based on those requirements.

Before you deploy configuration management technologies into your production environment, you must fully test your designs in a controlled test environment, and then review your test results to determine whether the systems meet the design requirements. It is strongly recommended that you stage your deployment of Group Policy and related technologies. For more information about staging, see “Staging Group Policy Deployments” in this book.

After you complete the testing of your design in a controlled environment, you can deploy to production. To learn about using the Windows Server 2003 Group Policy Management Console (GPMC) to facilitate testing and staging your deployments of Group Policy, see “Designing a Group Policy Infrastructure” in this book.

IntelliMirror Deployment Process

Deploying IntelliMirror configuration management technologies entails several processes. You begin your deployment plan by establishing your business objectives and identifying the resources to be managed, and then you define the scope of your project and evaluate your current environment in terms of the resources you need to manage and your requirements for configuration management technologies. Based on these requirements, you design managed configurations, determine the scope of application of your solution, test, and then stage and deploy your solution.

What this Guide Contains

Planning how you organize users and computers in Active Directory containers and how you apply Group Policy settings to manage them is an integral part of IntelliMirror. To help guide your design decisions for creating managed desktop configurations, you need a clear understanding of the appropriate technologies to use and the processes involved in implementing a desktop management solution that meets your business needs.

Although it is anticipated that you will read only those chapters in this guide that apply to your particular deployment needs, be aware that the IntelliMirror technologies rely on Group Policy and Active Directory for their delivery. Therefore, it is recommended that you read “Designing a Group Policy Infrastructure” in addition to the chapters that pertain to your particular deployment.

Each chapter is intended to assist you in planning, designing, testing, deploying, and implementing managed desktop configurations using IntelliMirror technologies.

Designing a Group Policy Infrastructure

Provides information about the process of defining your Group Policy objectives and designing a Group Policy infrastructure. Read “Designing a Group Policy Infrastructure” before you deploy Group Policy–based solutions that are described in other chapters in this book.

Staging Group Policy Deployments

Discusses the processes for creating and testing your Group Policy deployments in a controlled test environment. For example, “Staging Group Policy Deployments” explains how to create a test domain that mirrors a production domain by using the sample scripts provided with the Group Policy Management Console. You can perform incremental policy changes in the test environment, verify your changes, and then use the **Import** functionality of GPMC and migration tables to migrate the Group Policy objects (GPOs) you created to the production domain.

Deploying Security Policy

Discusses incorporating the Windows 2003 Server Group Policy security features into your overall security strategy to protect your corporate environment. “Deploying Security Policy” explains how to evaluate existing security policies, determine the level of risk acceptable for your environment, and deploy security policies.

Deploying Software Update Services

Discusses how to use Microsoft® Software Update Services (SUS) to collect, approve, and distribute critical Windows patches to resolve known security vulnerabilities and stability issues on computers running Windows XP; and Windows Server 2003 operating systems. “Deploying Software Update Services” guides you through the process of designing and deploying servers running SUS within your intranet.

Migrating User State

Discusses how to use the user state migration tools included in Windows Server 2003 to save and restore user data and settings when you move client computers to the Windows XP operating system from earlier versions of Windows. “Migrating User State” guides you through the processes of planning and implementing user state migration to conserve IT staff time, preserve important data, and minimize costs while maintaining user productivity.

Implementing User State Management

Discusses the processes involved in implementing user data and user settings management technologies to set up, manage, and control the availability of user data and personal settings across your network. IntelliMirror allows data and settings to be available to users even when their computers are disconnected from the network. “Implementing User State Management” helps you plan, test, and configure managed desktop configurations by using Roaming User Profiles, Folder Redirection, Offline Files and synchronization, and disk quotas and user profile quotas.

Deploying a Managed Software Environment

Discusses the process of deploying a managed software environment using the software installation extension of Group Policy. By using Group Policy–based software installation, you create a controlled environment that provides on-demand software installation and automatic repair of applications. “Deploying a Managed Software Environment” explains how to use Group Policy–based software deployment to manage software throughout all phases of the software administration life cycle.

Deploying a Simple Managed Environment

Discusses the process of combining the IntelliMirror technologies to create a simple managed environment. “Deploying a Simple Managed Environment” guides you through the steps required to deploy a complete IntelliMirror solution, which you can use as an initial production environment for a small organization, or a test environment for a larger organization.

Summary of Job Aids

As supplement to this book, you can use job aids, such as worksheets and checklists, which are designed to help you collect data for planning your configuration management deployments. Each worksheet is created for the type of information you need for planning, such as questions to answer, points to consider, and tables to help you organize your information. You can modify the designated job aids to develop your configuration management designs as appropriate for your organization’s needs. For worksheets to assist you with the deployment processes discussed in this book, see “Additional Resources,” later in this chapter.

Introduction to IntelliMirror Configuration Management Technologies

When you use Windows XP and Windows 2000 clients, and Microsoft® Windows® 2000 Server and Windows Server 2003 networks with Active Directory installed, you can take full advantage of IntelliMirror and Group Policy management features. Active Directory and Group Policy provide the foundation for IntelliMirror. Based on the Group Policy settings you specify, IntelliMirror can deploy, recover, restore, and replace user's data, software, and personal settings.

Table 1.1 lists the IntelliMirror core features, the technologies that enable these features, and the advantages of using IntelliMirror.

Table 1.1 IntelliMirror Features, Advantages, and Technologies

IntelliMirror Feature	Advantages	Technologies Used
User Data Management	Data is protected and highly available. Users can access their data from any computer on the network. For example, if you redirect specific user data folders, such as the My Documents folder, to a network location, and then making this location available to the users for offline use, users can access to their data wherever they log on. You can also manage configuration settings for Internet Explorer by using Group Policy.	Active Directory Group Policy Offline Files Folder Redirection Synchronization Manager Disk Quotas Enhancements to the Windows shell
User Settings Management	Users get their preferred desktop configuration from any computer on the network. Their preferences and settings for the desktop and applications are available wherever they log on.	Active Directory Group Policy Offline Files Roaming User Profiles Enhancements to the Windows shell
Computer Settings Management	You can use Group Policy to define options for computers, including security and network settings. For example, you can set options such as remote assistance, system restore, Windows file protection, and Terminal Services.	Active Directory Users and Computers snap-in Group Policy
Software Installation	You can centrally manage software installations, updates, repairs and removal.	Active Directory Group Policy Windows Installer

IntelliMirror Technologies

Active Directory and Group Policy together provide the foundation for IntelliMirror. The following technologies enable the IntelliMirror features.

Active Directory

Windows-based directory service stores information about objects on a network and makes this information available to administrators and users. By using Active Directory, you can view and manage network objects on their network from a single location, and users can access permitted network resources by using a single logon. The *Active Directory Users and Computers* Microsoft Management Console (MMC) snap-in is the recommended tool for managing Active Directory objects, including organizational units (OUs), users, contacts, groups, computers, printers, and shared file objects.

Group Policy

The infrastructure within Active Directory that enables directory-based configuration management of user and computer settings on computers running Microsoft® Windows® Server 2003, Standard Edition; Windows® Server 2003, Enterprise Edition; and Windows® Server 2003, Datacenter Edition operating systems and Windows 2000 and Windows XP Professional operating systems. The Group Policy settings that you create are contained in a Group Policy object (GPO). To create a GPO, use the Group Policy Object Editor snap-in for the MMC, which can be started from the Group Policy Management Console MMC snap-in (GPMC).

The GPMC tool provides unified management of all aspects of Group Policy across an enterprise, including cross-forest management. Using GPMC, you can manage all GPOs, Windows Management Instrumentation (WMI) filters, and permissions in your network.

GPMC consists of the following: a set of scriptable interfaces for managing Group Policy, the Group Policy Modeling Wizard for planning Group Policy deployments prior to implementing them in the production environment, the Group Policy Results Wizard for viewing GPO interaction and for troubleshooting Group Policy deployments, and a new MMC snap-in that gives you the ability to manage Group Policy across your organization through a single user interface.

For more information about Group Policy and GPMC, see “Designing a Group Policy Infrastructure” in this book.

You can download GPMC from the Microsoft Download Center; see the Group Policy Management Console link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>. You can use GPMC to manage both Windows 2000- and Windows Server 2003-based domains with Active Directory. By using GPMC to link a GPO to selected Active Directory system containers — sites, domains, and OUs — you can apply the GPO’s policy settings to the users and computers in those Active Directory containers.

You can use Group Policy to configure policy settings for the following:

Registry-based policy settings The Administrative Templates extension contains all registry-based policy settings, including those for the Windows 2000 or Windows Server 2003 operating systems and their components as well as any registry-based policy settings provided by applications. You use these policies to mandate registry settings that control the behavior and appearance of the desktop, the operating system components, and applications that provide registry-based policy.

Security settings You can set security options for computers and users within the scope of a Group Policy object. You can define local computer, domain, and network security settings.

Scripts You can use scripts to automate tasks when the computer starts and shuts down, and when the user logs on and logs off. You can use any language supported by Windows Scripting Host. These include the Microsoft Visual Basic® development system, Scripting Edition (VBScript), JavaScript, Perl, and MS-DOS®-style batch files (.bat and .cmd).

Folder Redirection You can redirect special folders on Windows 2000 Professional and Windows XP from their default user profile location to an alternate location on the network. These special folders include **My Documents**, **My Pictures**, **Application Data**, **Desktop**, and the **Start** menu.

Software installation You can centrally manage software in your organization. You can assign and publish software to users and assign software to computers.

Microsoft Internet Explorer Maintenance You can manage and customize Internet Explorer on computers running Windows 2000, Windows XP, and Windows Server 2003. You can also export settings for Microsoft® Windows® 95, Windows® 98, and Windows NT® version 4.0 clients (the settings are exported into an .ins and .cab file format for those platforms). Administrators can set options for browser user interface, connections, Uniform Resource Locators (URLs), proxy settings, security zones, and the **Favorites** folder and the **Links** bar.

Remote Installation Services Remote Installation Services (RIS) is used to control the behavior of the Remote Operating System Installation feature as displayed to client computers.

User profiles

A user profile describes the desktop computing configuration for a specific user, including the user's environment and preferred settings. The user profile is created when a user first logs on to a computer running Windows XP, Windows 2000, Windows NT, or Windows Server 2003. A user profile consists of a group of settings and files, which defines the environment that the system loads when a user logs on. It includes all the user-specific configuration settings, such as application settings, screen colors, network connections, printer connections, and mouse settings.

The following user profiles are available in Windows Server 2003, Windows XP, and Windows® 2000 Server and Microsoft® Windows® 2000 Professional:

- Local user profile. This is created the first time that a user logs on to a computer. The local user profile is stored on a computer's hard disk. Any changes made to the local user profile are specific to the computer on which the changes are made.
- Roaming user profile. A copy of the local profile is copied to and stored on a server share. This profile is downloaded every time that a user logs on to any computer on the network, and any changes made to a roaming user profile are synchronized with the server copy when the user logs off.
- Mandatory user profile. A type of profile that administrators can use to specify particular settings for users. Only system administrators can make changes to mandatory user profiles. Changes that a user makes to desktop settings are lost when the user logs off.

Offline Files

Offline Files complements Folder Redirection. By using Offline Files, users can disconnect from the network and continue working on the files as if they were still connected. When the computer is offline, the files and folders appear in the same directory as they do online — as if they still resided in the same location on the network. The user can then edit files even when not connected to the network. The next time the user connects to the network, the offline changes are synchronized with the network share.

Folder Redirection

By using Folder Redirection, users and administrators can redirect the path of a folder to a new location. The new location can be a folder on the local computer or a directory on a network share. Users can work with documents on a server as if the documents were based on the local drive. For example, you can redirect the **My Documents** folder (typically stored on the local hard disk) to a network location. The documents in the folder are available to the user from any computer on the network.

Synchronization Manager

When using Offline Files, users can use Synchronization Manager to synchronize all network resources. Users can set Synchronization Manager to automatically synchronize some or all resources. For example, users can set certain files and folders to be synchronized every time they log on or off the network. Synchronization Manager quickly scans the system for any changes, and if it detects changes, *only* the resources that have changed are updated, speeds up the synchronization process.

Disk quotas

You can set disk quotas to track and manage the amount of disk space used on the servers containing users' redirected folders. You can specify a disk quota limit and a disk quota warning level. If a user exceeds their designated quota limit, the user is prevented from storing additional files on the volume without first clearing some disk space. You can configure the disk quota system to log a system event when the users reach their quota warning level.

Software Update Services

SUS is a server component that you can install on a server running Windows 2000 or Windows Server 2003 to allow small and medium enterprises to bring critical updates from Windows Update inside their firewalls for distribution to computers running Windows 2000, Windows XP, and Windows Server 2003. You can use SUS to download the latest operating system patches to an intranet server, test the patches in your operating environment, select the patches you want to deploy to specific computers, and then deploy the patches.

User State Migration tool

If you are performing a large deployment of the Windows XP Professional operating system, use the User State Migration tool (USMT) to automate the migration of user state information. By using USMT, you can migrate users' personal display properties, folder and taskbar options, Internet browser and mail settings, as well as specific files or entire folders (such as **My Documents**, **My Pictures**, and **Favorites**) from their old computer to their new one. The USMT tool is included on the Windows Server 2003 CD in the \ValueAdd\Msft\USMT folder.

For more information about migrating user state information, see *Migrating User State* in this book. For more information about using USMT, see the User State Migration Tool link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Remote Installation Services

You can use RIS to install the base operating system on a new computer or to replace a system that has failed. By using RIS you can do such installations or replacements without visiting the individual computer. Clients must support remote booting by means of the Pre-Boot eXecution Environment (PXE) ROM. For client computers that do not have a remote boot-enabled ROM, you can use a remote-startup floppy disk; these clients must have a Peripheral Component Interconnect (PCI)-based network adapter.

You can centrally set client configuration options for Remote Installation Services by using Group Policy. The remote operating system installation feature uses Active Directory, Group Policy, Dynamic Host Configuration Protocol (DHCP), and RIS.

To facilitate computer replacement, you can use RIS to install the operating system, Group Policy-based software installation to recover applications, Roaming User Profiles to restore user profiles, and Folder Redirection to manage files centrally.

You can use IntelliMirror features separately or you can combine them depending on your business and organizational requirements.

IntelliMirror Implementation Examples

The examples that follow use some typical events at any organization to illustrate how the implementation of the IntelliMirror configuration management features in Windows Server 2003 impacts the computing environment. Example situations illustrate how the features and technologies of IntelliMirror can address typical desktop management needs.

Setting up the New Employee's Computer Example

A new user logs on to a new computer and finds documents and shortcuts already on the desktop. These shortcuts link to common files, data, and URLs that are useful to all users. Some examples of documents and shortcuts are the employee handbook or shortcuts to the user's departmental guidelines and procedures or to the intranet.

Also, if your computers come to you without an operating system, or if you have your own customized operating system installation, you can completely automate the installation of the client operating system for the new employee by using RIS. No technician is required to visit the computer. For more information about using RIS, see the Remote Installation Services (RIS) link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Implementing the Setting up of a New Employee's Computer Example

A default domain user profile and Group Policy are used to configure the new user's environment based on the user's job requirements. The administrator created a customized default domain profile that applies to all new domain users the first time they log on. When the users log on, they receive the customized settings from this profile. The advantage for the administrator of using a default domain profile is that all new users start from a base configuration that the administrator has chosen. Then, as the user personalizes the desktop settings, these settings are saved in the user's profile, which is stored either locally, or in a roaming user profile in a predetermined location on the network. By implementing roaming user profiles, you can provide the user with the required business information and settings whenever needed.

Logging on the First Time Example

A new employee logs on for the first time and sees that required software, such as Microsoft® Word, on the **Start** menu. When the new user selects Word on the **Start** menu, or double-clicks a Word document, Word is installed on demand.

Implementing a First Time Logon Example

Software Installation is implemented primarily through the use of Group Policy and the Windows Installerservice. Based on the user's Active Directory location and the Group Policy object applied, the user is assigned Word.

IntelliMirror ensures that the necessary and correct items assigned to the user appear in the **Start** menu. Using Group Policy, the administrator can assign or publish differently configured versions of the same application to different groups of users. When the user starts Word or opens an employee handbook in Word for the first time, the Windows Installer service checks to see if the application is installed on the local computer. If not, Windows Installer downloads and installs the necessary files for Word to run and sets up the necessary local user and computer settings. Although Windows Installer continues to check each time the application is invoked, it does not attempt to reinstall or repair the application unless necessary files are missing.

Making Offline Files Accessible to a Portable Computer Example

A portable-computer user working at the office creates a number of documents and saves them to the **My Documents** folder. After saving the documents, the user logs off, disconnects from the network, and takes the portable computer on a trip. While on the trip and off the network, the user continues to edit the documents saved earlier in **My Documents**.

Implementing Making Offline Files Accessible to a Portable Computer Example

In this situation, the documents are simultaneously saved to a network location and cached to the local computer in a process that is transparent to the user. This action takes place because the network folder is configured to be available offline. This configuration creates a copy of the network folder's contents on the local computer. The user can then access the data offline. By combining Offline Files with Folder Redirection, you can keep user data files backed up and secure on a centrally managed server. If a folder is both redirected and set to offline, that folder receives the benefits of being secure on a server drive, accessible by any computer the user logs on to, and remains available on the user's computer even if the network becomes inaccessible.

Returning to the Corporate Network

In this example, the user who uses a portable computer returns to the office and logs on to the network. Because the user made changes to files while working offline, a reminder balloon appears over the notification area showing that the changed files are being synchronized with the network files. In this situation, IntelliMirror technology identifies that the data in **My Documents** has changed and automatically updates the version on the network.

User Data Management and User Settings Management technologies are used to allow users to work on files offline and automatically update network versions of those files when they later reconnect to the network. Offline Files allows users to work on network files when not actually connected to the network. The Synchronization Manager coordinates synchronization of any changes between the offline version of a file and the network version.

Synchronization Manager helps you manage the multiuser use of network files. If multiple users modify the same network file, IntelliMirror notifies the users about the conflict and offers several resolution methods. The user can save the network version, the local version, or both versions. If both versions are to be kept, the user is asked for a new file name to store one of the versions.

Setting up a Shared Computer Environment Example

Users work in a department, such as a call center or IT support environment, where they use different computers from day to day. A user is working on a document late one night when the shift ends. The user saves the document and logs off the computer. The next day the user logs on to a different computer and connects to the network. The desktop has the same appearance and configuration as the computer used the previous night. The user resumes working on the same document that was saved in the **My Documents** folder the previous night.

Implementing Setting Up a Shared Computer Environment Example

A user's desktop was configured to use Roaming User Profiles so that a copy of the user's working environment was stored on a network server. When the user logged onto the computer, the user's existing preferences, shortcuts, and documents were copied to the local computer. The user was able to continue working as if using the original computer. A variation of this example is when one uses Roaming User Profiles in conjunction with Folder Redirection. This approach saves downloading time because the redirected folders do not need to be copied down to each computer. Users can have the same work environment and access to the same documents from any computer on the network. Changes that the user makes on one computer are synchronized with the other computer the next time the user logs on.

Replacing a Computer Example

The computer that a user is working on suddenly has a complete hardware failure. The user calls the technical support, and a new computer with only the Windows XP operating system installed arrives. Without further technical assistance, the user plugs in the new computer, connects it to the network, starts it, and can immediately log on. The user finds that the desktop has the same configuration as the computer it replaced — the same color scheme, screensaver, application icons, shortcuts, and preferences. More importantly, all the user's data files have been restored.

Implementing the Replacement of a Computer Example

IntelliMirror helps the user quickly get a computer installed and running with a minimum of support because data and settings are stored independently of any specific computer. By using Roaming User Profiles, Folder Redirection, and Group Policy, you can make the user's data, settings, and applications available wherever the user logs on to the network. In this example, the solution is not limited to getting the user a new computer. Instead, the user could also move to another computer in the office because all of the user's data, settings, and environment are mirrored on the network.

The features of IntelliMirror can be used separately or combined to address the range of needs, from minor configuration changes and updates to complete disaster recovery. This example only addresses IntelliMirror features. In this case, the support department shipped a computer that was preloaded with Windows XP Professional. However, by using RIS, it is also possible to send out computer hardware that has not been preloaded or configured. In that case, RIS can install Windows XP Professional after the computer is on site.

Implementing a Customized Home Page URL for all Domain Users Example

You are an administrator and you want to stipulate that the home page in Internet Explorer is configured to use the URL address of your organization's intranet home page for all domain users.

Implementing the Customized Home Page Example

In this example, a GPO is created, and policy settings are defined to use a customized home page URL. The GPO is linked at the domain level to ensure it applies to all users in that domain.

Managing Desktops in Non–Active Directory Environments

The availability of configuration management tools and features differs depending on whether your network operates exclusively in an Active Directory environment or in another network environment.

In a non–Active Directory environment, you can use other tools, such as Microsoft® Systems Management Server (SMS) for managing software distribution, the Internet Explorer Administration Kit for managing Internet Explorer settings, and System Policy (for Windows 95, Windows 98, and Windows NT 4.0) for managing registry-based settings. In addition, each local computer running Windows 2000, Windows XP Professional, Microsoft® Windows® XP 64-Bit Edition, or a Windows Server 2003 operating system has exactly one local Group Policy object (LGPO), even if it does not participate in a domain. Although it is possible to set a variety of settings by using the LGPO, the System Policy scales more easily to a large number of clients. The LGPO can be useful if you only need to apply certain settings to a small number of clients running Windows XP in a Windows NT 4.0 domain. Note that a local GPO does not support Folder Redirection or Group Policy–based Software Installation, and some security settings are not available in local GPOs.

Table 1.2 summarizes how desktop management tools differ between Active Directory and non–Active Directory environments.

Table 1.2 Desktop Management Tools and Features in Active Directory and Non–Active Directory Environments

Management Task	Active Directory	Non–Active Directory
Configure registry-based settings for computers and users	Administrative templates deployed by using Group Policy Administrative templates, deployed using local Group Policy object (LGPO)	System Policy LGPO
Manage local, domain, and network security	Security settings deployed by using Group Policy Security Settings deployed LGPO	LGPO
Centrally install, update, and remove software	SMS Group Policy–based software distribution	SMS
Manage Internet Explorer configuration settings after deployment	Internet Explorer Maintenance in the Group Policy Object Editor snap-in Internet Explorer Maintenance deployed by using LGPO Internet Explorer Administration Kit (IEAK)	LGPO IEAK

(continued)

Table 1.2 Desktop Management Tools and Features in Active Directory and Non-Active Directory Environments (*continued*)

Management Task	Active Directory	Non-Active Directory
Apply scripts during user logon/logoff and computer startup/shutdown	Logon/logoff and startup/shutdown scripts can be centrally configured in Group Policy or independently by using the LGPO	LGPO
Centrally manage users' folders and files on the network	Folder Redirection in conjunction with Offline Files and Folders	System Policy Manipulation of registry settings
Centrally manage user settings on the network	Roaming User Profiles	Roaming User Profiles (for Windows domains)

Developing a Deployment Plan

To use the IntelliMirror technologies for managing configurations effectively, you must develop a plan that defines the resources to be managed and the management processes to be implemented. To ensure the success of your deployment of the technologies for managing configurations, you need to do the following:

- Analyze your organization's current configuration management process. When you develop your configuration management infrastructure, determine how your organization currently manages its computing environment.
- Determine goals for your managed environment deployment. As you begin your design process, establish the criteria that define the success of your managed environment project. The business requirements of the various organizational groups of users may differ, and success, therefore, means different things to each group. For example, a system administrator might consider a project successful if it results in a reduction in the ten most common support calls, although for a department manager, success includes increased user productivity. It is important that you set achievable and measurable goals, and that you review them periodically to track your progress.
- Design your solution for configuration management by using the IntelliMirror technologies to meet your business requirements.
- Follow a process to implement a configuration management infrastructure. Analyze your business requirements, service level agreements, security, network, and IT requirements, and then determine the appropriate technologies to use to meet your requirements. By following the guidelines in this book for designing your configuration management infrastructure, you can establish the approach that best suits your organization's needs.

- Create a configuration management team. The majority of change and configuration management deployments are likely to have cross-functional boundaries, so as part of preparing your deployment, it is important to consult with various functional teams in your organization and ensure they participate during analysis, design, test, and implementation phases as appropriate.

A recommended option is to use the Microsoft Solutions Framework (MSF) team model. In the MSF model, small multidisciplinary teams are created, and team members share responsibilities to focus on the project.

You can align your team with the MSF model by including the six roles in the change and configuration management design team.

- *Product Management.* Ensures the goals of the project are met.
- *Program Management.* Facilitates the team and manages resources.
- *Development.* Designers and implementers of the CCM infrastructure.
- *Testing.* Ensures all issues are known before the release of the design.
- *Logistics Management.* Treats physical requirements of the deployment.
- *User Education.* Designs user and team training materials.

For more information about the Microsoft Solutions Framework Team Model, see the Microsoft Solutions Framework link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Defining the Scope of Your Configuration Management Project

It is important to identify both the organizational and the technical scope for your configuration management deployment. The primary purpose is to deploy a configuration management infrastructure to meet the needs of a defined set of users and to manage a clearly defined computing environment. Defining the scope is important both to set user expectations and concrete goals for the project.

Organizational Scope

To understand the configuration management requirements of an organization, you need to identify the organizational structure and determine organizational goals.

You can create a map of your organization to show a representation of its logical hierarchy (an organizational chart). This chart is useful as an input to the design process as it defines natural boundaries within the business, which might function as separation points in the use of IntelliMirror technologies. The breakdown of the organization's resources includes all levels of job roles. Use the job roles as input when you categorize users by job type.

Resources to be Managed

The technical scope for deploying a configuration management infrastructure involves all computing resources to be managed, including hardware and software.

It is useful to develop a diagram of the network to serve as a logical representation of servers and services within the network. Work with the network administrators and the Active Directory deployment team to obtain this information. The diagram needs to illustrate the following information:

- Location of domain controllers and member servers
- Site configuration
- Link speed within and across sites
- Servers that provide specific services, such as Domain Naming Services (DNS) and DHCP
- Interfaces with infrastructure elements outside the scope of configuration management, such as firewalls, networking equipment, and systems running other operating systems

Use the network diagram to indicate which components of the computing environment are to be managed by the configuration management infrastructure and which components are to remain unmanaged.

Assessing Your Current Environment

Assessing your current environment is the first step toward identifying how IntelliMirror can meet your desktop management needs. To identify the areas where IntelliMirror can provide the most benefit for your organization, examine how you perform your desktop management tasks. For example, evaluate how your IT staff handles common desktop management situations such as the following:

- New applications that need to be made available to users as quickly as possible.
- Users who move from one location to another and must retain access to their primary applications and data even on a different computer.
- Users who travel frequently and have intermittent network access, sometimes over slow links.
- New employees who require a newly configured computer that includes all their required applications.
- Users who receive new computers and need to have an operating system installed, along with their applications and data.

Use this process as a starting point to define the tasks your IT group performs for configuration management. You need to determine:

- How your organization currently performs the tasks associated with change and configuration management
- How your organization currently manages desktops

After you determine how your organization manages desktops, you can create a flowchart or table to identify the most common and frequently occurring desktop management tasks that your IT department performs.

Evaluating Your Desktop Management Processes

Analyzing your current configuration management processes helps you to identify ways you can improve service and reduce your total cost of ownership (TCO).

You need to assess your desktop environment and evaluate the current methods your organization uses for installing operating system, applications and service packs. You also need to evaluate the backup processes in place and determine the level of security to provide for desktops.

For a worksheet to help you evaluate your desktop environment, see “Worksheet A.4 Assessing Your Current Desktop Environment” (DMEUSE_4.doc) on the *Microsoft® Windows® Server 2003 Deployment Kit* companion CD (or see “Worksheet A.4 Assessing Your Current Desktop Environment” on the Web at <http://www.microsoft.com/reskit>).

Large organizations typically support hundreds of software applications as well as multiple versions of operating systems. To help reduce the cost associated with client computing, you can implement standards for corporate-wide software such as virus protection, e-mail, word processing, and spreadsheets—and then retire obsolete or unnecessary software.

To develop your client application standards, examine the operating system types and the versions your organization has installed, the commercial applications your organization uses (such as word processing software), and the line-of-business applications that your corporation has developed for tasks such as managing clients or filling orders. For a worksheet to help you assess your organization’s software standards, see “Worksheet A.5 Evaluating Software Standards” (DMEUSE_5.doc) on the Windows Server 2003 Deployment Kit companion CD (or see “Worksheet A.5 Evaluating Software Standards” on the Web at <http://www.microsoft.com/reskit>).

Evaluating Computer and User Roles

It is recommended that you configure a user's environment according to the user's job or role in the organization. You can then specify the security and other configuration settings for different types of computers such as member servers and desktops. The Group Policy settings you define for each group of users and computers should be based on their business requirements.

Domain controllers and member servers

If you have different types of member servers, such as Microsoft® Exchange 2000 Server, terminal servers, or file and print servers, it is likely that you need to define and create different Group Policy objects to configure the settings on each type of server. For example, when managing terminal servers, you need to ensure that you apply user settings Group Policy based on the *computer* that the user logs on to. To achieve this, consider using the Group Policy setting for loopback policy processing. (The **User Group Policy loopback processing mode** policy setting is an advanced option that applies user settings based on the location of the computer object.)

To simplify troubleshooting and problem solving, place the domain controllers and the different types of member servers into separate organizational units and allocate Group Policy objects accordingly.

Desktops

Different computers require different policy settings based on their roles. To support these differences, you need to create Group Policy objects that configure each computer according to its role.

To use IntelliMirror to create configurations for computers, you need to consider things such as whether a given computer is configured to allow multiple users to log on. You also need to determine if the computer retains or discards user profiles between user sessions and if the computer provides local storage space for copies of offline files.

Categorizing Users by Job Types and Location

Categorizing users in your organization according to their job requirements, computer experience, and location is an important part of the process of developing Group Policy objects for managing the various desktop configurations users require.

Several user types can be used to describe the majority of job roles in most organizations. Every user has specific job-based needs for data management, and users often have multiple roles. For example, a high-performance user might also perform the tasks of a knowledge user.

For each user category, consider what type of configuration options to allow users to make on their computers. Determine if users should run with User or Power User privileges, whether users can install software, or make desktop configuration changes. For example, you might allow high-performance users to change the desktop colors, and you probably want to prevent data-entry workers from making any desktop configuration changes.

High-performance users

High-performance users — engineers, graphic artists, and software developers, for example — rely on information technology (IT) to do jobs that are often project- or process-driven. They typically require highly specialized applications.

It is recommended that such users store their data on corporate servers even though they might also need access to local storage on a disk for performance. However, local data is not backed up. Users need permanent access to their data regardless of their location.

Knowledge workers

Knowledge users require IT to collect data from many sources, convert the data into information, and communicate the information to support decision-making transactions. Knowledge workers' jobs are typically project-driven, requiring both personal productivity and specialized applications. For example, this category includes executive staff, financial analysts, consultants, researchers, and reporters.

Knowledge workers mainly store data on corporate servers. Users tend to share their working data with others in their department or with those working on the same project.

Process workers

Process workers — in customer service, claims and loan processing, for example — use IT to add value to a process. These users perform repetitive process-driven tasks, which require personal productivity and your organization's customized applications.

These users' data is typically stored on corporate servers, and they might have limited write-access to the local computer. In some cases, it might be appropriate to use a fully locked-down desktop.

Data-entry workers

Data-entry jobs — processing airline reservations, making order entries, and typing transcriptions — require IT to transcribe data from one medium to another and to add value to data by making it available for other uses.

Data-entry users have no access to disk drives, CD-ROM drives, or the local file system, and their data is stored on corporate servers. Users might share workstations with users on other shifts or with temporary workers.

In addition to categorizing users according to their IT service requirements, you need to identify them by the locations from which they access the corporate network to perform their jobs. Location categories are largely independent of the user types already defined in this section.

Stationary users

Stationary users access the corporate network by using local area network (LAN) links. Their computers have permanent LAN connections and high-speed links to connect to the users' data on local servers. The nature and volume of the users' work is fairly predictable. Therefore, their needs for IT services can be easily anticipated.

Roaming users

Roaming users access the corporate network by using LAN links. They have permanent LAN connections when working locally, but if they roam between sites, they might have restricted network bandwidth back to some servers. They need to access their data from multiple workstations from many different areas in the same physical location.

Mobile users

Mobile users need to access the network at different times and locations by dial-up connections, varying LAN connections, or across a wide area network (WAN) link. Therefore, network services must be accessible at any time.

The following characteristics apply to mobile users:

- Their computers are often connected by slow or intermittent network links.
- The bandwidth, quality, and consistency of their network connections are highly variable.
- Users data and settings need to be saved locally when the users work offline. The users' data and settings might be synchronized to a file server.
- The availability of different types of services depends on whether the users are connected to the corporate network and on the speed and reliability of their connections.

Remote users

Remote users are occasionally connected by slow or intermittent network links, but they connect by using the same link each time. They need access to the corporate network at their convenience. Therefore, network services must be accessible at any time. Users need to save data and settings locally, which might not be synchronized to a file server.

Two other important considerations to take into account when analyzing your users and your organization for desktop management are security and corporate policy. You need to consider how you can protect your desktops from possible security threats. Also, you need to consider how your desktop management plans might affect the corporate culture. For more information, see “Determining Corporate Policies” later in this chapter.

Evaluating Your Security Requirements

The security requirements for managed desktops in your organization are an essential part your configuration management deployment. Examine both the internal and the external security threats that might exist. Internal threats range from accidental damage that your users might cause to their desktops to intentionally malicious actions. External threats include viruses, hackers, or persons with malicious intent. Some things to consider as you plan for desktop security include:

- What user security level is appropriate for users to have on their computers?
Three fundamental levels of security are granted to users by membership in one of these groups: Users, Power Users, and Administrators. Membership in the Users group gives the most protection from a number of external threats, such as viruses, and it limits the damage that a user can accidentally or intentionally cause to their computers. However, user level permissions have the most incompatibility problems with older applications. Take particular care before you give users privileged access to computers that they share with other employees.
- What type of systems do the workstations need to interoperate with?
They might need to interoperate with Windows NT 4.0 servers, UNIX server message block (SMB) servers, or other types of servers. Interoperability with older systems means that some security you might use in a pure Windows Server 2003 environment must be relaxed.
- Do users have to provide any level of support on their own computers, or do they have to configure their own computers?
Users who use portable computers and provide their own support might require administrator rights on their computers. Other high-performance users, such as developers, might also need administrative rights.

A series of security templates is supplied with Windows Server 2003 that you can use to manage security configurations. For more information about deploying Windows Server 2003 security, see “Deploying Security Policy” in this book or see “Planning a Secure Environment” in *Designing and Deploying Directory and Security Services* of this kit.

Determining Corporate Policies

Desktop management has both political and technical consequences. Depending on the current corporate policy and the culture of your organization, implementing restrictive desktop configurations can either be straightforward or complicated. Often, the more centralized the current IT structure and standards are, the easier it is to gain user acceptance of more restrictive desktop configurations. For example, organizations that have implemented system policies in Windows NT 4.0 to configure common managed desktops might find that users accept quite restrictive policies in Windows 2000 and later. However, organizations moving from an unmanaged Windows NT 4.0 environment (or from a Windows 95 or Windows 98 environment) might encounter resistance to increased restrictions. This can delay or challenge your efforts to impose new or restrictive managed configurations.

This does not mean that an organization with a distributed administration and policy structure cannot benefit from IntelliMirror desktop management. The majority of IntelliMirror features are not readily visible to the user, and many — such as Offline files and application publishing, for example — are enabling rather than restricting technologies. You can actually save time and resources by taking time to carefully examine the benefits of imposing a particular restriction and weigh it against the potential costs of resistance. Where the benefits outweigh the costs, you might want to think about a user education program (as part of the migration training) so that users understand the motivation behind the policy settings.

For more information educating users, see “Preparing Users for Deployment” later in this chapter.

Assessing Network and Storage Requirements

The availability of network bandwidth can affect how Group Policy settings are applied. It is also important to have sufficient network bandwidth available between servers and workstations when you deploy Roaming User Profiles, Offline Files, and Folder Redirection. Collecting information about your network infrastructure and network traffic patterns helps you plan your deployment of IntelliMirror technologies.

To plan for disk space allocation, you need to determine the disk storage that the users and computers in your organization require.

Evaluate Your Network Infrastructure

Evaluate how your network infrastructure meets your user-demand for bandwidth. If some of your users connect to your network over slow or intermittent communication links, the placement of your distribution points and other servers assumes even greater importance in your planning. Determine if any areas of your network are problematic. Where remote users are highly managed, you might justify the cost of upgrading the communication link. By default, when Windows Server 2003 detects a slow link, it does not apply all Group Policy objects to the remote user or computer. For example, security settings and administrative templates are applied, but software installation and scripts are not. The reliability and speed of your local- and wide-area communication links influence your placement of servers and the management functionality you are able to offer to users.

Offline Files, Folder Redirection, and Roaming User Profiles all transfer data files across your network. Software installation sends applications. By testing and piloting, you can best determine the amount of data that passes over your network as a result of implementing these technologies.

The central networking questions you need to answer when deploying IntelliMirror include:

- What changes do you need to make in the physical, logical, and site topology of your network to support these technologies?
- Does your network have the correct protocols to support these technologies?
- Is your network bandwidth within and between sites sufficient to support IntelliMirror features?

You also need to collect the following data:

- The number of clients at each location served. Correlate the placement of servers, routers, and domain controllers to the clients serviced by each device. Remember to include mobile clients.
- Configuration information about network devices such as modems, routers, and hubs. Note whether your routers are configured to pass on broadcast packets. This information is useful when deciding where to place software distribution points.

Evaluate Your Network Traffic Patterns

Because IntelliMirror operations involve sending information across your network, knowing the pattern and load of network traffic is essential for planning. Collect the following data about your network traffic patterns:

- Bandwidth demands such as peak utilization and percentage utilization.
- Usage patterns. Establish whether all users log on and off at the same time, or whether user logon time is spread more evenly.

You can estimate the network load generated by software installation by noting:

- Whether installation of the software is mandatory (assigned) or optional (published), and whether the assignment is to a user or to a computer.
- The size of the software package that is installed.
- The placement of the software distribution point in relation to the targeted users.

If you assign software to a computer, the software installation takes place when the computer is restarted. When you perform large deployments to groups of computers, the workload on your network increases substantially when the users start their computers. Consider performing such deployments so that you minimize disruptions to users.

Assigning software to be available on-demand to a user places a shortcut to the software on the user's **Start** menu, but the software is not actually installed until the user starts the application. You can also use the **Install this application at logon** option to install software the next time the user starts the computer, or after the user logs off and then back on. To some degree the load is spread out as users install the software whenever they require it. However, in the case of large-scale deployments to many users, a significant number of users might install the assigned software within the same time period. You can spread out demand on bandwidth over time by publishing software to users so that each user decides when or if to install the package.

You also need to consider the impact of Roaming User Profiles and Folder Redirection on the network loads. If possible, try to minimize the bandwidth impact of synchronizing user data and profiles to network file servers by placing the servers so that data traveling back and forth is localized to the network segment instead of traveling over your entire network or across slow links.

Evaluate Storage Requirements

When implementing IntelliMirror technologies, you need to allocate server storage space to hold user data and settings. Allocating server storage space for user data and user settings is complicated by the variety of files (both in number and size) that each user stores on a network server. You need to determine the following:

- Type of user you are supporting
- Typical desktop environment in your organization
- IntelliMirror technologies you are deploying

Recording this information helps you estimate how much server storage space you need to allocate for user data and profiles.

Although you can use Disk Quotas to limit the amount of server disk space available to each user, you can also choose to set a limit but not enforce it. In that case, Windows Server 2003 logs a system event whenever a user uses more than the specified amount of disk space. You can then examine the logs to estimate the amount of disk space that you need for storing user data and settings.

To calculate your server capacity needs when you use Folder Redirection, begin by listing the folders you need to redirect to the network. For example, you can redirect any of the following folders for each user: **My Documents** folder, **Desktop**, **Application Data** folder, and the **Start** menu. Then determine how much local disk space your users' data consumes in the specified folders. You can gather this information by writing scripts (VBScript, WMI queries, or Perl, for example). Or you can use other inventory tools to gather file size data, filtering for the specified directories and known data files extensions such as .doc and .xls. Use this information to estimate the server storage space needed for Folder Redirection.

If possible, minimize the impact on bandwidth of synchronizing user data and profiles to network file servers. To do this, place the servers so that the data traveling back and forth is localized to the network segment, instead of traveling over your entire network or across slow links. Track and control the total number of users saving data files to each server, and track how much data is being stored.

You can control the disk space used to store user data and settings by imposing disk quotas or controlling the size of a user's profile. You can monitor and enforce the size of a user's profile by setting profile quotas. If a user's profile is larger than the size you specify, the user is prevented from logging off until the user reduces the amount of disk space used by that profile. Testing and piloting IntelliMirror features on a sample group of users can provide valuable information about the average and median profile size of your users.

If you use Roaming User Profiles while redirecting the **My Documents** folder of your roaming users, you might not want to impose profile quotas. The reason is that files such as custom dictionaries (size outside user's control) are written to the user profile. Imposing profile quotas can frustrate users who cannot control the size or number of files in their profile.

Evaluating Service Level Agreements

Many IT organizations find that the best way to maintain service level agreements with various departments within an organization is to structure services by levels. For example, an organization might define service level agreements (SLAs) that specify the maximum amount of time allowed for the logon screen in Windows 2000 to appear (when the workstation is turned on) or for the user to have access to the desktop after successfully logging on.

You might categorize your services by basic and custom services. *Basic services* are a predetermined set of services you agree to provide to a business unit for a specified cost. You can have several levels of basic services, each with its own assigned cost. Basic services might include standard hardware and software configurations for desktop computers.

Custom services are additional specialized services that a business unit might request. When a business unit requests custom services, you have a specified charge-back rate for them. Custom services might include special software configurations created for a user with unique needs.

Determining Your Requirements for Configuration Management Technologies

To ensure that your design supports the administrative requirements of your organization, begin by determining your organization's current administrative practices and the existence of any administrative boundaries, technical or political, that might impact the design. To determine your specific administrative requirements, you can ask a number of questions about the current configuration management tasks and methods, document the responses, and collect data. This will help you define the goals of your configuration management infrastructure.

Evaluate the administrative tasks you currently perform when installing operating systems, managing user settings and data, computers, and software distribution.

Operating System Installations

Assess how your organization manages operating system installations and upgrades, including the following:

- Number of operating system installations that are performed per month
- Frequency of operating system upgrades
- Time to install or upgrade a client computer
- Automation processes used to reduce the time required for installations or upgrades

User Settings and Data Management

Managing user settings requires that you assess the levels of control users need to have over their environment and how user profiles are stored. If a policy is currently in place, determine the business requirements it meets.

When you examine the organizational requirements for user data and settings management, determine whether a different strategy can improve user productivity and reduce the need for IT intervention.

Managing user data requires that you consider which configuration management technologies can be implemented to improve the process of managing user data. To do this, document your requirements for the following:

- Backup procedures for user data
- Types of users who regularly use more than one computer and ways that improved data access can enhance their job performance
- Amount of time and money spent recovering and recreating data when hardware or software problems cause a computer failure
- Potential amount of lost revenue to the organization if a catastrophic loss of user data occurs
- Need for users to take server-based data with them off site. Mobile and remote users have different requirements due to the transient nature of their network connections and distance from support staff.

Computer Settings Management

Analyze the administrative tasks you currently perform to manage computer settings, such as security and network configuration settings. You need to ensure that you provide appropriate, secure computer configurations based on the business requirements of your organization. You should evaluate issues such as user authentication, access to resources, and network settings.

Authentication and access to resources Determine how users are currently authenticated to the network and their computers, what resources users are permitted to access, and to which groups they belong. By using Group Policy, you can define security settings to manage multiple computers. You can create a security policy by importing a security template to a Group Policy object. Security settings include options for administering the following: account policies, local policies, Event log settings, membership in restricted groups, startup and permissions for system services, and registry and file system access control list (ACLs) permissions.

You can also specify policy settings for IPSec, software restriction policies, public key policies, and wireless network (IEEE 802.11) configurations.

Administrative rights requirements Determine whether the users have to configure and support their own computers. For example, users who have to provide their own support (such as users who use portable computers) might require administrator rights on their computers. Other high-performance users, such as developers, might also need to use administrative rights.

Interoperability in mixed server environments Determine the type of systems with which the users' workstations need to interoperate, such as Windows NT 4.0 servers, UNIX server message block servers, or other types of servers. To support interoperability with older systems means that some security settings you might use in a pure Windows 2000 environment must be relaxed.

Network settings Determine whether you need to set up specific network settings on a per-computer basis — DNS or proxy settings, for example.

Scripts Determine the types of scripts to use when a computer starts or shuts down. You can use both VBScript (.vbs) and JScript (.js) scripts.

Internet Explorer maintenance To manage Internet Explorer settings for computers, you can use Group Policy for the following: security zones, proxy settings, controlling the installation of Internet Explorer components by users, and displaying or hiding the Internet Explorer splash screen.

Users privileges on the local computer Establish whether a user, or set of users, should be a member of the Users, Power Users, or Administrators group.



Note

Typically, for security purposes, it is *not* recommended that users log on to their computers with administrative credentials. If users need to perform administrative tasks on their computer, the users can use the **Run as** command to perform such tasks.

Software Distribution

Evaluate the current methods your organization uses for deploying and managing software throughout the software lifecycle. Include the following considerations:

- How applications are deployed, whether the methods used are adequate, and whether the software distribution is too wide in its scope.
- How applications are used, and the common support issues that arise.
- How often applications are upgraded, and how upgrades are performed.
- How applications are removed, and whether full removal is achieved.

For more information about managing configurations by using IntelliMirror technologies, see the following chapters in this book:

- “Designing a Group Policy Infrastructure” for information about deploying Group Policy to manage groups of users and computers.
- “Implementing User State Management” for information about managing user data and user settings.

- “Deploying Security Policy” for information about managing security settings.
- “Deploying a Managed Software Environment” for information about using Group Policy to deploy software.
- “Deploying Software Update Services” for information about using Microsoft SUS to manage the deployment of Windows patches.

After you identify your business needs, you can determine which features are most useful for your organization.

Identifying the IntelliMirror Technologies That Meet Your Configuration Management Needs

You can use the following IntelliMirror technologies to improve your configuration management processes:

- User data management
- User settings management
- Computer settings management
- Software management
- Remote operating system installations

User Data Management

Ensuring that data remains available is a leading concern for most organizations. What happens to user data when a hard disk fails? Who ensures that users back up their files on a timely basis? Too often, user data backups are not performed, and important files are lost if the user’s hard disk fails.

Other concerns include the availability of user’s data, whether or not users have access to their data if they move to a different computer on the network, or if they are only intermittently connected to the network. Using the appropriate IntelliMirror desktop management technologies, you can ensure that users can access their data from any computer wherever they log on, whether online or offline. You can back up user data centrally and provide fast computer replacement in disaster recovery situations.

By using IntelliMirror to manage user data, you provide the following advantages:

- You can provide improved protection of user data by ensuring that local data is also redirected or copied to a network share, providing a central location for administrator-managed backups. This capability helps to enforce corporate directives such as to place all important data on servers.
- You can ensure that the most up-to-date versions of a user's data reside on both the local computer and on the server. Local caching maintains data on the local computer even when it is not connected to the network. This ensures that data is available to the user, even when the user is working offline.
- When a user roams to another computer on the network, the user's data can follow. This provides increased accessibility because users can use any computer on the network to access their data.

Implementing user data management relies on some or all of the following technologies:

- Active Directory
- Group Policy
- Roaming User Profiles
- Folder Redirection
- Offline Files
- DFS (Distributed File System)
- EFS (Encrypting File System)
- Disk quotas

For more information about how to implement user data management technologies, see “Implementing User State Management” in this book.

User Settings Management

In most organizations, new and existing users who change computers often need help from the IT department initially to configure their computers. By using the IntelliMirror technologies to manage user settings, you can centrally define computing environments for groups of users and computers so that users automatically get the correct configurations for their jobs. You can also restore user settings if a computer fails to ensure that a user's desktop settings follow the user if they roam to another computer.

By managing user state, you can accomplish the following:

- Reduce support calls by providing a preconfigured desktop environment appropriate for the user's job.
- Save time and cost for computer replacement.
- Help users work more efficiently by providing a consistent, secure, preconfigured desktop environment, no matter where they work.

The settings you can manage include:

- Desktop configurations
- Security settings
- Language settings
- Application settings
- Scripts (for when a computer starts or shuts down and when a user logs on or logs off)

Administrators can also redirect any of the special folders in a user profile to a network share. Then the same user profiles are available wherever a user logs on.

User settings, like user data, can follow the user regardless of where that user logs on. Administrators use settings to customize and control users' computing environments and to grant or deny the users the ability to customize their own computing environments. These settings can be applied to both users and computers. When users have permission, they often customize the style and default settings of their computing environment to suit their needs and work habits. Settings contain three basic types of information: user and administrative information, temporary information, and data that is specific to the local computer. For example:

- User settings include items such as Internet Explorer favorites, quick links, cookies, and the Microsoft® Outlook® Express personal Web address book or background bitmap.
- Temporary information includes items such as the user's personal Internet Explorer cache.
- Local computer settings include items such as the folders and files marked for offline use.

You use the following technologies to implement user settings management:

- Active Directory
- Group Policy
- Offline Files
- Synchronization manager
- Folder Redirection
- Roaming User Profiles

For more information about how to implement User Settings Management, see "Implementing User State Management" in this book.

Computer Settings Management

Group Policy provides numerous settings to help you manage the computers and servers in your organization. By using Group Policy, you can manage the following types of settings for computers:

Security settings

You configure security settings on computers to protect resources on the computers or the network.

Account policies Defined on computers, they determine how user accounts interact with the computer or the domain. This includes password policy for domain or local accounts, account lockout policy, and Kerberos policy.

Local policies Include audit policy, user rights policy, and security options.

Public key policies Includes Encrypting File System policy settings.

Software restriction policies Used to protect your computing environment by identifying and specifying which applications are allowed to run on computers.

Internet Protocol security Provides protection against private network or Internet attacks. IPSec uses cryptographic security services to ensure private, secure data transmission over Internet Protocol (IP) networks.

Scripts

You can specify scripts to run when the computer starts up or shuts down.

Windows components

You can specify policy settings for NetMeeting, Internet Explorer, Task Scheduler, Terminal Services, Windows Installer, and Windows Messenger.

System

You can specify policy settings for **User Profiles**, **Scripts** (to determine how scripts run), **Logon**, **Disk Quotas**, **Net Logon**, **Group Policy** (to specify how Group Policy should be processed), **Remote Assistance**, **Error Reporting**, **Windows File Protection**, **Remote Procedure Call**, and **Windows Time Service**.

Network

You can specify policy settings for **DNS Client**, **Offline Files**, **Network Connections**, **QoS Packet Scheduler**, and **SNMP**.

Printers

You can specify policy settings for printers such as allowing printers to be published to or deleted from Active Directory or Web-based printing.

Software Management

User productivity is enhanced when users have all of the software applications that enable them to perform their jobs efficiently. It is also important that IT tracks applications that are no longer being used, or are out of date, and makes sure those are phased out. The IT group determines when to stop supporting software that is no longer useful. In some cases, the best solution is to remove the obsolete application instead of risk compatibility issues and other problems that can result from its continued use.

Application management tasks can be extremely labor intensive. That is why many organizations want to automate them for large groups or even for all client computers at one time.

Microsoft provides several software deployment solutions. By evaluating your business objectives for deploying software, the types of requirements your solution must meet, and the types of client operating systems in your organization, you can determine the most appropriate method for deploying software.

Group Policy–based software installation

You can use Group Policy–based software installation to install software applications when a computer is started, when the user logs on, or on demand. This approach is suitable for small and medium organizations that have deployed Active Directory, and whose client computers are Windows 2000 Professional or later. You can also use Group Policy–based software installation to upgrade deployed applications or remove earlier applications that are no longer required. You can ensure that a user cannot install any software from local media, such as a CD-ROM, or disk, or other unapproved applications.

The Group Policy–based software installation feature also provides for the following situations:

- If a user inadvertently deletes files from an application, the application repairs itself.
- If a user moves from one computer to another, the software remains available to the user.
- If an application is not installed on a user's computer, and the user tries to open a document associated with that application, the application is automatically installed and the document opens.

You can apply software installation policy settings to users or computers in your Active Directory structure. You can also use Group Policy to set software restrictions to help protect the computer environment from questionable or unknown software.

Group Policy–based software installation does have some basic limitations, including the inability to schedule installation, manage network bandwidth, or provide feedback on the status of the installation. Consider using Systems Management Server if you need to provide scheduled installations, manage network use, perform hardware and software inventory, or monitor installation status.

For more information about deploying software by using Group Policy–based software installation, see “Deploying a Managed Software Environment” in this book.

Systems Management Server

SMS is appropriate for medium and large organizations that use client computers running Windows 2000 or earlier. SMS does not require Active Directory. SMS provides advanced capabilities such as inventory-based targeting, status reporting, server- and client-side scheduling, multisite facilities, complex targeting, centralized hardware and software inventory, remote diagnostic tools, software metering, software distribution-point population and maintenance, support for Windows 95, Windows 98, Windows NT 4.0, Windows 2000, and Windows XP clients, and enhanced software deployment features.

For more information about SMS, see the Microsoft Systems Management Server link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Software Update Services

SUS is a method for quickly acquiring and distributing critical Windows patches to computers in your organization. You can use Software Update Services to download the latest critical or security patches, test the patches, and efficiently deploy the patches to the appropriate computers. You can use these services on computers running the following operating systems: Windows 2000, Windows XP, and Windows Server 2003.

For more information about using Software Update Services, see “Deploying Software Update Services” in this book.

Remote Operating System Installations

You can use the Remote Installation feature to perform a new installation of Windows on Preboot eXecution Environment (PXE) remote boot-enabled client computers throughout your organization. An administrator does not have to visit the new computer to install a new operating system and core applications. You can provide a customized, fully automated installation process from a remote source. When the computer is turned on, the user presses F12 to initiate the operating system installation process. The computer then starts from a network server that supports RIS.

You can use RIS servers using RIsetup and RIPrep to deploy all editions of Windows 2000 (except Microsoft® Windows® 2000 Datacenter Server), Windows XP Professional, and all editions of Windows Server 2003 (except Windows Server 2003, Datacenter Edition). You can also use RIS servers using RIsetup to deploy Windows XP 64-Bit Edition and the 64-bit versions of Windows Server 2003.

You use the following technologies to implement Remote Installation:

- Active Directory
- Group Policy
- DNS
- DHCP
- RIS

Designing Managed Configurations

Many help desk calls occur after users attempt to upgrade and install nonstandard hardware and software. By creating standards, and designing and deploying managed configurations in your organization, you can specify which applications users can access and which features are available, based on users' job types, services provided by the IT department, and the needs of your corporate environment.

You can limit unnecessary access to system functionality to decrease the number of problems users might inadvertently cause. For example, you can use Group Policy to prevent users from accessing various storage devices such as floppy disk drives, hard disks, or CD-ROMs. By using security policy or ACLs, you can also secure objects, such as system files and the registry, so that your users cannot gain access to them.

Implementing standard configurations can result in increased user productivity by reducing the incidence of computer-related problems. Also, because standard configurations are easier to troubleshoot or replace, they bring about a reduction in support costs.

Mapping Managed Configurations to User and Computer Roles

After you categorize users by their job requirements and locations, and determine the types of servers and clients in your organization, you can determine how best to combine these categories with other organizational considerations to create managed configurations for your organization.

Managed configurations can be mapped to the user categories as described in “Categorizing Users by Job Types and Location” earlier in this chapter. You can design configurations to address the specific business requirements of your organization.

The following examples illustrate how you can use IntelliMirror features to create managed configurations.

Highly Managed

Use the highly managed configuration for process workers whose work requires highly restricted configurations with only a few applications. This configuration is suitable for marketing, processing claims and loans, and serving customers.

A highly managed desktop has the following characteristics:

- Users working different shifts can share the computer. Each user needs a unique logon account.
- Users can customize a limited number of application-specific settings.
- Users can access their data from any computer.
- User data is stored on server shares, and users do not store data locally

Table 1.3 lists the features that you can use to design a highly managed configuration.

Table 1.3 Features Used for a Highly Managed Configuration

Feature	Comments
Roaming User Profiles	User settings are available at any computer on the network to which the users log on. You can remove cached copies of the roaming user profile when the users log off by using Group Policy.
Folder Redirection	Redirect My Documents to a network share.
Offline Files	Designated files are cached locally to ensure that in event of network disconnection, the users can continue to work on these important files.
Software installation	Core applications are installed on all laptops (these applications are assigned). Optional applications are available for users to install locally (these applications are published).
Disk quotas	You can use disk quotas on the servers that contain redirected folders so that individual users cannot use excessive amounts of disk space.
Software installation	You can assign core applications to users. Optional applications are available for users to install locally (these applications are published).
Security context and template	User or Power User. The secure workstation security template is used as the basis for this configuration.

Lightly Managed

Use for high-performance users who require a lot of control over their computers, in an organization where highly managed desktops are not acceptable to users, or where desktop management is highly delegated.

The lightly managed desktop has a minimal set of restrictions that help reduce desktop support costs and user down time:

- Users can customize most settings that affect them but are prevented from making unauthorized system changes.
- Users can log on to any computer on the network and access their data.
- User data is saved on server shares and is not stored locally.

Table 1.4 lists the features that you can use for creating a lightly managed configuration.

Table 1.4 Features Used for Configuring a Lightly Managed Configuration

Feature	Comments
Roaming User Profiles	Users get the same settings on any computer they use.
Redirected Folders and Offline Files	Any files that you redirect must also be set as offline files, so that the users can continue to work on their files even when their computer is not connected to the network.
Software Installation	Core applications are installed on all laptops (these applications are assigned). Optional applications are available for users to install locally (these applications are published).
Disk quotas	Use disk quotas on the servers that contain redirected folders so that individual users cannot exhaust available shared disk space.
Security context and template	User or Power User. The secure workstation security template is used as the basis for this configuration.

Mobile User

A mobile user configuration is appropriate for managing *mobile users* — traveling users who often use portable computers. Mobile users typically log on to the same computer, and they connect by both high speed and low speed.

The following characteristics apply to mobile-user desktops:

- Can be configured so that users have access to user data whether the computer is connected to or not connected to the network.
- Can save data locally or on network servers.
- Can be configured so that users can disconnect from the network without logging off or shutting down, and to have data files synchronized automatically.

Table 1.5 summarizes the configuration management features you can use to create a mobile user configuration.

Table 1.5 Features Used for a Mobile User Configuration

Feature	Explanation
User profiles	<p>Use the following criteria to determine which type of profile to use:</p> <ul style="list-style-type: none"> • If the user regularly connects to the network by using a fast link and if you want to back up user state or they use multiple computers, use a roaming user profile. • If the user rarely connects by a fast link, use a local profile. • If the user roams to LAN-connected computers in the domain and also has a portable computer, use a roaming user profile.
Folder Redirection	<p>Redirect the My Documents folder so that users can access centrally stored data and documents from anywhere. Redirected folders are automatically made available offline, to provide access when users are not connected to the network.</p>
Ability for user to customize	<p>Permit customizations within certain guidelines so that users can personalize their work environment but are prevented from making changes to critical system settings.</p>
Software installation	<p>Core applications are installed on all laptops. Administrators assign these applications. Optional applications are available for users to install locally (these applications are published).</p>
Group Policy settings	<p>Use Group Policy settings to create the managed environment.</p>
Security context and template	<p>User or Power User.</p> <p>The highly secure workstation security template is used as the basis for this configuration.</p>

Multiuser

The multiuser desktop is appropriate for environments such as a university laboratory, public computing center, or a library where users might be allowed to save some customizations, such as desktop wallpaper and color scheme preferences, but are prevented from changing hardware or connection settings.

A multiuser configuration has the following characteristics:

- The system is mostly restricted, but some personal settings are allowed.
- Users can log on and use a configured roaming profile.
- Users share this computer with other users either by having a unique logon account or by using a Guest account.
- User data is saved on server shares, and users do not store data locally.

Table 1.6 lists the features you can use for a multiuser configuration.

Table 1.6 Features of a Multiuser Configuration

Feature	Comments
Multiple users	Users share this computer. Each user has a unique logon account.
Roaming User Profiles	Makes user settings available from any computer and enables administrators to easily replace computers without losing their configuration. When the user logs off, the local cached version of the profile is removed to preserve disk space.
Folder Redirection	User data is saved on server shares and Group Policy is set to prevent users from storing data locally. Redirect My Documents, Desktop, and Application Data.
Ability for user to customize	Most of the system is locked down, but some personal settings are available.
Assigned applications	Core applications common to all users are assigned to the computer. Other applications are available for on-demand install by means of user assignment.
Published applications	Applications are available for users to install from Add or Remove Programs in Control Panel.
Group Policy settings	Group Policy settings are used to create the managed environment.
Security context and template	User. Based on the highly secure workstation security template.

Kiosk

The term *kiosk* in this context refers to a public workstation that runs only one application and one user account, runs unattended, and automatically logs on. Users are unknown to the kiosk owner and do not provide logon credentials. A kiosk workstation is highly secure, simple to operate. Users can not change the default settings.

Use the kiosk desktop in a public area where multiple users access the computer or where you want to prevent users from making any customizations. For example, the kiosk is frequently used in airports where passengers check in and view their flight information.

The following characteristics apply to the kiosk desktop:

- The system is highly restricted by applying policy settings.
- Users cannot customize the installed applications.
- Users cannot save data to the computer locally or to the network.
- The computer can be in a stand-alone environment without any network connectivity.
- Users cannot add or remove applications.
- Users are anonymous, and all users share the same user account.

Table 1.7 lists the features you can use for a kiosk configuration.

Table 1.7 Features of a Kiosk Configuration

Feature	Comments
User profile type	Local.
Folder Redirection	Not used.
Ability for user to customize	No user customizations are permitted. Use policy settings to prevent users from accessing the Taskbar and Start menu.
Assigned applications	One application is assigned to the computer.
Security context and template	User. The highly secure workstation security template is used as the basis for this configuration.

Task Station

Use the *task station* desktop — an entry terminal for orders on a manufacturing floor or in a call center, for example — for data entry workers when you need dedicated computers to run a single application.

A task station configuration has the following characteristics:

- The computer is dedicated to running a single application.
- Users on different shifts often share computers.
- Each user has a unique logon account.
- Many users roam between multiple computers that run the same single application.
- User data is saved on server shares and can be stored locally.

Table 1.8 lists the features you can use to configure a task station desktop.

Table 1.8 Features of a Task Station Configuration

Feature	Comments
Multiple users	Users share this computer. Each user has a unique logon account.
Roaming User Profiles	Makes user settings available from any computer and enables administrators to easily replace computers without losing their configuration. When the user logs off, the local cached version of the profile is removed to preserve disk space.
Folder Redirection	Redirect My Documents and Application Data.
Ability for user to customize	No user customizations are permitted. You can also use policy settings to prevent users from accessing the Taskbar and Start menu.
Assigned applications	Typically one application is assigned to the computer. No published applications are made available for users to install.
Security context and template	User. The highly secure workstation security template is used as a basis for this configuration.

Configurations for Computer Replacement

To simplify computer replacement and to minimize interruption to users, you can store the user data and settings independently of any specific computer. By using Roaming User Profiles and Folder Redirection, you can ensure that the users' data, settings, and applications are available wherever the users log on.

You can also simplify setting up a new managed computer on your network by using RIS to create standardized operating system configurations. You can create a customized image of a Windows XP Professional or Windows 2000 Professional desktop from a source computer. You can save that desktop image to the RIS server, and then use that preconfigured image to set up multiple desktops. You can only include the operating system in the image or a pre-configured desktop image that includes both the operating system and a standard, locally installed desktop application.

Designing Your Organizational Unit Structure

When you plan your configuration management solution, ensure that you design an OU structure that facilitates the management of Group Policy.

The OU hierarchy does not need to mirror your organization's departmental hierarchy. Create every OU to have a defined purpose, such as delegation of authority or application of Group Policy. Business needs must drive the OU hierarchy. By delegating administrative authority, you can designate groups of users to have control over the users and computers or other objects in an OU. An OU is the smallest Active Directory container to which you can assign Group Policy settings.



Note

Redirusr.exe (for user accounts) and **redircomp.exe** (for computer accounts) are two new tools included with Windows Server 2003 to assist with the application of Group Policy to new user and computer accounts. These tools are located in %windir%\system32. New user and computer accounts are created in the CN=Users and CN=Computers containers by default. It is not possible to apply Group Policy directly to these containers. By running Redirusr.exe and Redircomp.exe once for each domain, the domain administrator can specify OUs into which all new user and computer accounts are placed at the time of creation. This allows administrators to manage these unassigned accounts by using Group Policy *before* the administrators assign them to the OU in which they are finally placed. It is recommended that the OUs used for new user and computer accounts be highly restricted by means of linked GPOs to increase security around new accounts.

For more information about redirecting the Users and Computers containers, see article Q324949, "Redirecting the Users and Computers Containers in Windows Server 2003 Domains," in the Microsoft Knowledge Base. To find this article, see the Microsoft Knowledge Base link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

For more information about the **redirusr.exe** and **redircomp.exe** tools, see the Redirecting Users and Computers link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Application of Group Policy

You can link GPOs to sites, domains, and OUs to implement Group Policy settings as broadly or as narrowly in the organization as necessary. Keep in mind how Group Policy is applied when you determine the scope of application of Group Policy objects:

- The policy settings in Group Policy objects are inherited, cumulative, and apply to all users and computers in an Active Directory container.
- Group Policy objects are processed in the following order: local GPO, site, domain, and OU.
- By default, Group Policy inheritance is evaluated starting with the Active Directory container farthest from the computer or user object. The Active Directory container closest to the computer or user overrides Group Policy set in a higher-level Active Directory container unless you set the **No Override** option for that GPO.
- If you link more than one GPO to an Active Directory container, the GPO processing order (priority) is as follows: the GPO highest in the **Group Policy Object Links** list, displayed in the Group Policy page of the Active Directory container's **Properties** page, has precedence by default. If you set the **No Override** option in one or more of the GPOs, the highest GPO that is set to **No Override** takes precedence.

For information about creating an Active Directory structure see “Designing the Active Directory Logical Structure” in *Designing and Deploying Directory and Security Services* of this kit.

For more information about defining the scope of application of Group Policy, see “Designing a Group Policy Infrastructure” in this book.

Testing Your Configuration Management Design

Before deploying your management solutions to a wide base, fully test your design in a test lab environment. Minimally, your test environment consists of at least two domain controllers, a member server, two or more workstations, and possibly a mobile computer connected by means of a slow link. If you are testing software installation through Group Policy, include one or more servers set up as software distribution points. By setting up a test-to-production environment deployment process and using features of the Group Policy Management Console, you can ensure that you provide a reliable and consistent configuration management solution.

Document the testing network as well as all steps required to set it up. If new hardware, such as a new server, is being added to your organization's network, use this same hardware in your test deployment if possible.

To minimize variables and to ensure that testing does not interfere with your organization's network services, keep the testing network on its own, isolated LAN.

**Note**

If there is a network server that you cannot simulate, such as a database service, you might need to temporarily connect the testing network to the organization's network to verify that the deployment interacts with this service as expected. Use this approach *only* if you have no other options available for verifying the interaction of the deployment with the service.

After completing tests in a controlled environment, select a group of users to pilot your configuration. Keep the users to a manageable number. A pilot can expose unexpected problems on a small scale so that you can resolve them before deploying on a large scale. Verify that the deployed technology is operating as expected. If you perform an iterated deployment, deploy and test it in phases, and then emphasize the testing of the final configuration.

You can perform two types of testing:

- Proof of concept testing
- Pilot testing

When conducting such tests, be prepared to iterate if necessary. Depending on the scope of any design updates, you might want to repeat the proof of concept or pilot stage before proceeding further.

Conducting Proof of Concept Testing

Proof of concept testing provides the opportunity to try out a design in a controlled environment and to identify any potential major problems or challenges prior to conducting a pilot with users.

Use a Test Environment Conducting a proof of concept test requires a test environment that can be configured to simulate the intended configuration for your production environment. Typically, this is a small-scale simulation that is also large enough to demonstrate the core structures and policy settings that you have designed.

Primary aspects of conducting a proof of concept test are to give a representative sample of users and administrators access to the test environment and to confirm that the design meets their requirements and expectations.

Involve the Design Team Ensure that all members of the design team have the opportunity to review the Proof of Concept and are confident that it meets the design objectives.

Conducting Pilot Testing

You can conduct a pilot test to try out a design with a controlled number of users. This enables you to capture refinements that have not been identified during the design phase, and to highlight any issues that have not previously been seen during the proof of concept phase. In some circumstances, you can use pilot testing to check system performance and resilience under real-user conditions. Carrying out a pilot test involves tasks, starting with selecting the appropriate users.

Selecting the appropriate users Typically, it is good practice to select users who have volunteered to participate in the pilot, instead of imposing the test on them. Volunteer users are more likely to be fully involved in the pilot, and take the time to test the configurations.

Providing pre-pilot training In any pilot, it is essential to provide adequate user training before deploying the system, and to set expectations about what is required from the users during the test phase. For example, you need to tell users who to contact if they encounter problems and how to provide feedback.

Deploying the pilot When deploying the pilot, it is good practice to involve any implementation team that is required to implement the final systems. The team can then identify issues in advance and plan how to solve them.

Reviewing and refining After conducting the pilot, perform a review of the process to ascertain whether the systems met the design requirements. This helps you identify any improvements you need to consider for inclusion in the final design.

For more information about how to stage, test, and deploy your configuration management deployments, see “Staging Group Policy Deployments” in this book.

Preparing Users for Deployment

Desktop management changes the way many users interact with their computers. It might also change how they access their data, where their settings are stored, how they install software, and which software they can access. As you begin to implement new desktop management standards, it is important to develop a plan to educate and support your users.

If you create standard desktops, you need to let users know well in advance what changes are planned and how you plan to implement those changes. In addition, you need to train users, as well as IT and support staff, to use the new features. Resources that users can refer to for information when questions arise, such as a corporate Web site or newsletter, can help to ease the transition.

You also need to think about how users might perceive your new management processes. For example, a common phrase many IT professionals use to describe a highly managed desktop is “locked down.” Although system administrators and IT professionals understand this phrase, many users might not like the idea of the IT department locking down their desktops. As you train your users, emphasize how a managed environment provides value. For example, users are likely to appreciate the convenience of automatic software installation and repair.

You also need to determine how you will provide user support during the transition. As you begin to implement new features, determine what percentage of your staff will support upgraded users and the escalation procedures the support staff will use. Make sure to document the problems that users encounter as you implement different parts of your plan. That information helps you support the next set of users.

Staging and Deploying Your Design to the Production Environment

The importance of staging your deployments of Group Policy can not be overemphasized. After you have performed incremental policy changes in the test environment and verified your changes, you can begin to migrate the Group Policy objects you created to your production domain by using the migrate functionality and the migration tables included in GPMC.

As you begin to implement desktop management services in your organization, look for the desktop management technology that provides the greatest benefit to your organization. Implement that service before you begin to implement others. This gives you the opportunity to test one set of technologies relative to the technologies already in place before you implement another set.

For example, you might decide that protecting and backing up user data would provide the greatest benefit to your organization. You might then choose to implement Folder Redirection in your company so that all user data is centrally stored on a server, facilitating backup. After you deploy Folder Redirection to your users, you can reevaluate whether additional IntelliMirror technologies such as Roaming User Profiles or Software Installation and Maintenance is appropriate to implement next.

By following the processes described in “Staging Group Policy Deployments” in this book, you can ensure that you provide a predictable, consistent configuration management solution.

Additional Resources

These resources contain additional information and tools related to this chapter.

Related Information

- “Deploying a Simple Managed Environment” in this book for an example of how IntelliMirror technologies are used to create a simple managed environment for your users.
- “Designing the Active Directory Logical Structure” in *Designing and Deploying Directory and Security Services* of this kit.
- The *Distributed Services Guide* of the *Windows Server 2003 Resource Kit* (or see the *Distributed Services Guide* on the Web at <http://www.microsoft.com/reskit>) for more information about Group Policy.

- “Designing RIS Installations” in *Automating and Customizing Installations* of this kit.
- “Designing a Group Policy Infrastructure” in this book.
- “Staging Group Policy Deployments” in this book.
- “Deploying Security Policy” in this book.
- “Deploying Software Update Services” in this book.
- “Migrating User State” in this book.
- “Implementing User State Management” in this book.
- “Deploying a Managed Software Environment” in this book.
- “Deploying a Simple Managed Environment” in this book.

Related Job Aids

- “Worksheet A.1 Identifying Primary Client Support Tasks” (DMEUSE_1.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.1 Identifying Primary Client Support Tasks” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.2 Assessing User Data Management Tasks” (DMEUSE_2.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.2 Assessing User Data Management Tasks” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.3 Assessing User Settings Management Tasks” (DMEUSE_3.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.3 Assessing User Settings Management Tasks” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.4 Assessing Your Current Desktop Environment” (DMEUSE_4.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.4 Assessing Your Current Desktop Environment” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.5 Evaluating Software Standards” (DMEUSE_5.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.5 Evaluating Software Standards” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.6 Analyzing Your Users by Job Function” (DMEUSE_6.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.6 Analyzing Your Users by Job Function” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.7 Classifying Your Users” (DMEUSE_7.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.7 Classifying Your Users” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.8 Managing Different Types of Users” (DMEUSE_8.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.8 Managing Different Types of Users” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.9 Evaluating your Security Requirements” (DMEUSE_9.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.9 Evaluating Your Security Requirements” on the Web at <http://www.microsoft.com/reskit>).

- “Worksheet A.10 Considering Common Configurations” (DMEUSE_10.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.10 Considering Common Configurations” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.11 Training Needs for Various Workers” (DMEUSE_11.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.11 Training Needs for Various Workers” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.12 Updating Network Documentation” (DMEUSE_12.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.12 Updating Network Documentation” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.13 Documenting Servers (Example)” (DMEUSE_13.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.13 Documenting Servers (Example)” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.14 Documenting Client Computers” (DMEUSE_14.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.14 Documenting Client Computers” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.15 Documenting Clients (Example)” (DMEUSE_15.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.15 Documenting Clients (Example)” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.16 Evaluating Network Infrastructure” (DMEUSE_16.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.16 Evaluating Network Infrastructure” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.17 Documenting Network Infrastructure” (DMEUSE_17.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.17 Documenting Network Infrastructure” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.18 Evaluating Network Traffic Patterns” (DMEUSE_18.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.18 Evaluating Network Traffic Patterns” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.19 Monitoring Network Performance with System Monitor” (DMEUSE_19.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.19 Monitoring Network Performance with System Monitor” on the Web at <http://www.microsoft.com/reskit>).

Designing a Group Policy Infrastructure

2

Microsoft® Windows® Server 2003 Group Policy enables administrators to manage configurations for groups of computers and users, including options for registry-based policy settings, security settings, software deployment, scripts, folder redirection, Remote Installation Services, and Microsoft® Internet Explorer maintenance. By using Group Policy, you can significantly reduce an organization's total cost of ownership. Because of factors such as the large number of policy settings available, the interaction between multiple policies, and inheritance options, Group Policy design can be complex. By carefully planning, designing, and testing a solution based on your organization's business requirements, you can provide the standardized functionality, security, and management control that your organization needs.

In This Chapter

Group Policy Overview	52
Planning Your Group Policy Design	58
Designing Your Group Policy Model	68
Deploying Group Policy.....	82
Maintaining Group Policy	115
Additional Resources.....	117

Related Information

- For more information about the Active Directory® directory service, see the *Directory Services Guide* of the *Microsoft® Windows® Server 2003 Resource Kit* (or see the *Directory Services Guide* on the Web at <http://www.microsoft.com/reskit>).
- For more information about security in Windows Server 2003, see the *Distributed Services Guide* of the *Windows Server 2003 Resource Kit* (or see the *Distributed Services Guide* on the Web at <http://www.microsoft.com/reskit>).
- For more information about managing Group Policy, see the *Distributed Services Guide* of the *Windows Server 2003 Resource Kit* (or see the *Distributed Services Guide* on the Web at <http://www.microsoft.com/reskit>).

Group Policy Overview

Group Policy enables Active Directory–based change and configuration management of user and computer settings on computers running a member of the Microsoft® Windows® Server 2003 or Microsoft Windows® 2000 families of operating systems, or the Microsoft® Windows® XP Professional operating system. You use Group Policy to define configurations for groups of users and computers, including policy settings for registry-based policies, software installation, scripts, folder redirection, Remote Installation Services, Internet Explorer maintenance, and security. You can also use Group Policy to help manage server computers, by configuring many server-specific operational and security settings.

The Group Policy settings that you create are contained in a Group Policy object (GPO). To create a GPO, use the Group Policy Management Console (GPMC). To edit a new GPO, use the Group Policy Object Editor snap-in for the Microsoft Management Console (MMC), which you can start from GPMC. By using GPMC to link a GPO to selected Active Directory system containers — sites, domains, and organizational units (OUs) — you apply the policy settings in the GPO to the users and computers in those Active Directory containers.

To guide your Group Policy design decisions, you need a clear understanding of your organization’s business needs, service level agreements, and security, network, and IT requirements. By analyzing your current environment and users’ requirements, defining the business objectives you want to meet by using Group Policy, and following this chapter’s guidelines for designing a Group Policy infrastructure, you can establish the approach that best supports your organization’s needs.

To see example standard desktop configurations and the actual policy settings used for those configurations, see the Group Policy scenarios in the whitepaper at the Implementing Common Desktop Management Scenarios link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>. For a list of these sample configurations, see Table 2.3 later in this chapter.

IntelliMirror refers to the ability to provide users with consistent access to their applications, application settings, roaming user profiles, and user data, from any managed computer – even when they are disconnected from the network. IntelliMirror is delivered by means of a set of Windows features that enable IT administrators to implement standard computing environments for groups of users and computers.

IntelliMirror can significantly boost user productivity and satisfaction by doing the following:

- Allowing users to continue working efficiently in intermittently connected or disconnected scenarios by enabling uninterrupted access to user and configuration data under these conditions.
- Delivering a consistent computing environment to users from any computer when their desktop or laptop computer is unavailable or in scenarios where users are not assigned a specific computer.
- Minimizing data loss by enabling centralized backup of user data and configuration files by the IT organization.
- Minimizing user downtime by enabling automated installation and repair of applications.

Implementing IntelliMirror also boosts administrator efficiency and reduces IT costs by doing the following:

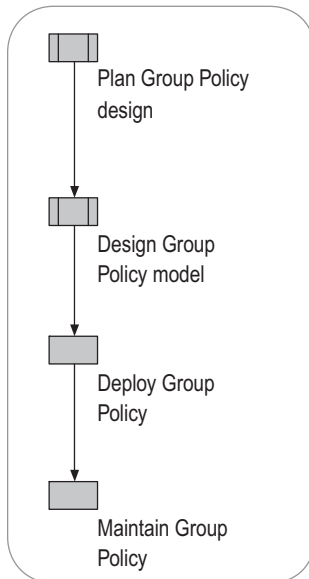
- Eliminating the need to manually configure user settings, install applications, or transfer user files to provide users access to their computing environments on any computer.
- Enabling scenarios where users do not have an assigned computer but log in to any available computer in a pool of computers. This helps reduce hardware and administration costs.
- Easing the IT task of implementing centralized backup of user files while satisfying the need for these files to be available on the user's computer.
- Reducing support costs by using Windows Installer to automatically repair broken application installations.
- Enabling rapid deployment of security settings to ensure resources on the network are secure.

Windows features that implement IntelliMirror include Active Directory, Group Policy, Software Installation, Windows Installer, Folder Redirection, Offline Folders, and Roaming User Profiles.

Process for Implementing a Group Policy Solution

The process for implementing a Group Policy solution entails planning, designing, deploying, and maintaining the solution. These steps are illustrated in Figure 2.1.

Figure 2.1 Implementing Group Policy



When you plan your Group Policy design, make sure that you design the OU structure to ease Group Policy manageability and to comply with service level agreements. Establish good operational procedures for working with GPOs, such as those defined in this chapter, make sure that you understand Group Policy interoperability issues, and determine whether or not you plan to use Group Policy for software deployment.

During the design phase, define the scope of application of Group Policy, determine the policy settings that are applicable to all corporate users, classify users and computers based on their roles and locations, and then plan desktop configurations based on the user and computer requirements.

The deployment phase begins by staging in a test environment. This includes creating standard desktop configurations, filtering the scope of application of GPOs, specifying exceptions to default inheritance of Group Policy, delegating administration of Group Policy, evaluating effective policy settings by using Group Policy Modeling (formerly known as Resultant Set of Policy planning mode), and evaluating the results by using Group Policy Results (formerly known as Resultant Set of Policy logging mode).

Staging is critical. Thoroughly test your Group Policy implementation in a test environment before deploying to your production environment. After you complete staging and testing, migrate your GPO to your production environment by using GPMC. Consider an iterative implementation of Group Policy: rather than deploying 100 new Group Policy settings, initially stage and then deploy only a few settings to validate that the Group Policy infrastructure is working well.

Finally, prepare to maintain Group Policy by establishing control procedures for working with and troubleshooting GPOs by using GPMC.

What You Need Before Designing Your Group Policy Solution

Before designing your Group Policy implementation, you need to understand your current organizational environment, and you need to take preparatory steps in the following areas:

Active Directory Ensure that the Active Directory OU design for all domains in the forest supports the application of Group Policy. For more information about Active Directory OU design, see “Designing the Active Directory Logical Structure” in *Designing and Deploying Directory and Security Services* of this kit.

Group Policy Management Console (GPMC) Download and install the Group Policy Management Console, which consists of scripting interfaces and a Microsoft Management Console snap-in.

Networking Make sure that your network meets the requirements for change and configuration management technologies. Because Group Policy works with fully qualified domain names, you must have DNS running in your forest in order to correctly process Group Policy; you cannot use NETBIOS only. Also, because client or destination computers must be able to contact your network’s domain controllers, do not turn off the ICMP protocol. If destination computers cannot ping the domain controllers, Group Policy processing will fail.

Security Obtain a list of the security groups currently in use in your domain. Work closely with the security administrators as you delegate responsibility for organizational-unit administration and create designs that require security-group filtering. For more information about filtering GPOs, see “Applying GPOs to Selected Groups (Filtering)” in “Defining the Scope of Application of Group Policy” later in this chapter.

IT requirements Obtain a list of the administrative owners and corporate administrative standards for the domains and OUs in your domain to develop a good delegation plan and to ensure that Group Policy is properly inherited.



Note

Turning off the ICMP protocol will cause Group Policy processing to fail. Turning off Read access on Active Directory containers that are in the hierarchy of a user or computer object will cause Group Policy processing for that object to fail.

Administrative Requirements for Group Policy

To use Group Policy, your organization must be using Active Directory and the destination desktop and server computers must be running Windows 2000 Professional, Windows 2000 Server, Windows XP Professional, or Windows Server 2003. You can manage server computers as well as client computers by using Group Policy; Group Policy offers many settings specific to server computers.

Using GPMC will greatly improve the manageability of your Group Policy deployment and enable you to take full advantage of the power of Group Policy by providing an enhanced and simplified Group Policy management interface.

By default, only domain administrators or enterprise administrators can create and link GPOs, but you can delegate this task to other users. For more information about administrative requirements for Group Policy, see “Delegating Administration of Group Policy” later in this chapter.

New in Windows Server 2003: Group Policy Management

GPMC is a new tool that unifies management of all aspects of Group Policy across multiple forests in an enterprise. GPMC allows you to manage all GPOs, Windows Management Instrumentation (WMI) filters, and Group Policy-related permissions in your network. Think of GPMC as your primary access point to Group Policy, with all the Group Policy management tools available from the GPMC interface. The information presented in this book is based on using GPMC for Group Policy deployment and ongoing management.

GPMC consists of a set of scriptable interfaces for managing Group Policy and an MMC-based user interface (UI). The UI integrates all previous Group Policy tools into a unified Group Policy-management console. GPMC runs on 32-bit computers that are running a member of the Windows Server 2003 family operating system or Windows XP Professional with Service Pack 1 and the Microsoft® .NET Framework. This tool can manage both Windows Server 2003 and Windows 2000 Active Directory–based domains.

GPMC provides the following:

- A new user interface that integrates existing Group Policy functionality currently accessible by using various tools such as the Active Directory Users and Computers snap-in, the Active Directory Sites and Services snap-in, the Delegation of Control Wizard, the RSoP snap-in, the Delegation Wizard, and the ACL editor. The UI also simplifies inheritance and enforcement of GPOs.
- Access to the Group Policy Object Editor (previously known as the Group Policy MMC snap-in).

- Importing and exporting GPOs.
- Copying and pasting GPOs.
- Backing up and restoring GPOs.
- Searching for existing GPOs.
- Integration of RSoP capabilities:
 - Group Policy Modeling. Allows you to simulate RSoP data for planning Group Policy deployments prior to implementing them in the production environment.
 - Group Policy Results. Allows you to get RSoP data for viewing GPO interaction and for troubleshooting Group Policy deployments.
- Support for migration tables to facilitate cross-domain and cross-forest GPO import and copy operations.
- Reporting GPO settings and RSoP data in HTML reports that you can save and print.
- Scripting all operations that are available within the tool. You cannot, however, use scripts to edit individual policy settings in a GPO.

**Note**

To help you get started, the GPMC installation includes sample scripts that use COM interfaces. The sample scripts are installed in the folder `\Program Files\GPMC\Scripts\`.

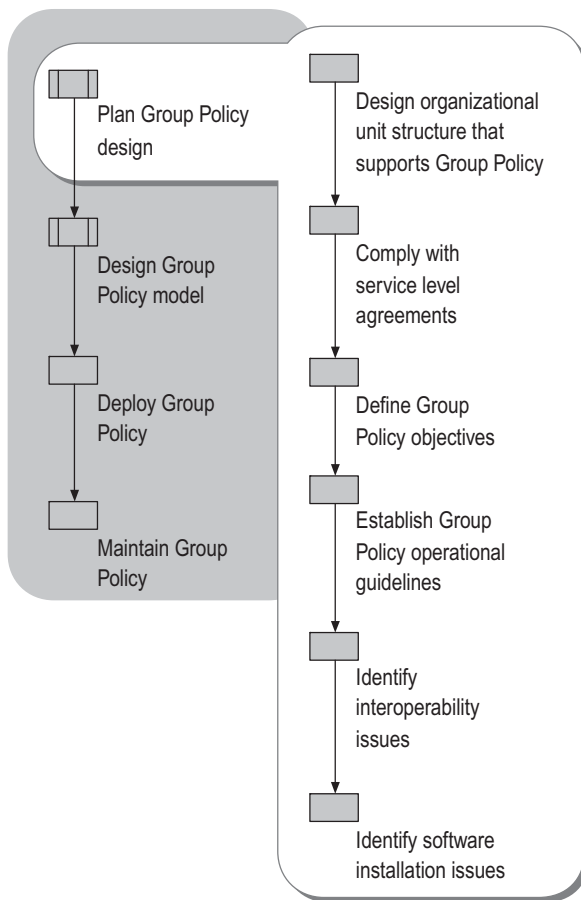
GPMC deployment and troubleshooting operations are described throughout this chapter. For detailed, step-by-step information about using GPMC to deploy and manage your Group Policy infrastructure, see Help in GPMC. Full details of the scripting interfaces are documented in the Group Policy Management Console Software Development Kit (SDK), which is located at program files\gpmc\scripts\gpmc.chm on any computer where you install GPMC. The GPMC SDK is also available in the Microsoft® Platform SDK. For more information and to download SDKs, see the Microsoft Platform SDK link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Before you begin planning your Group Policy design, install GPMC. It is available as a download from the Microsoft Web site. See the Group Policy Management Console link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Planning Your Group Policy Design

When you plan your Group Policy design, ensure that your Active Directory design supports the application of Group Policy. Then you need to clearly define your objectives for deploying Group Policy. Specifically, understand any service-level agreements and administrative issues that pertain to Group Policy and consider your business requirements and how Group Policy can help you achieve them. Finally, incorporate any operational, interoperability and software installation considerations into your plan. Figure 2.2 illustrates the steps in the Group Policy planning process.

Figure 2.2 Group Policy Planning



Designing an OU Structure that Supports Group Policy

In an Active Directory environment, you assign Group Policy settings by linking GPOs to sites, domains, or organizational units (OUs). Typically, most GPOs are assigned at the organizational unit level, so be sure your OU structure supports your Group Policy-based client-management strategy. You might also apply some Group Policy settings at the domain level, particularly those such as password policies, which only take effect if applied at the domain level. Very few policy settings are likely to be applied at the site level. A well-designed OU structure, reflecting the administrative structure of your organization and taking advantage of GPO inheritance, simplifies the application of Group Policy. For example, it can prevent needing to duplicate certain policies so that the policies can be applied to different parts of the organization, or having to link the same GPO to multiple Active Directory containers to achieve your objectives. If possible, create OUs to delegate administrative authority as well as to help implement Group Policy.

OU design requires balancing requirements for delegating administrative rights – independent of Group Policy needs – and the need to scope the application of Group Policy. The following OU design recommendations address delegation and scope issues:

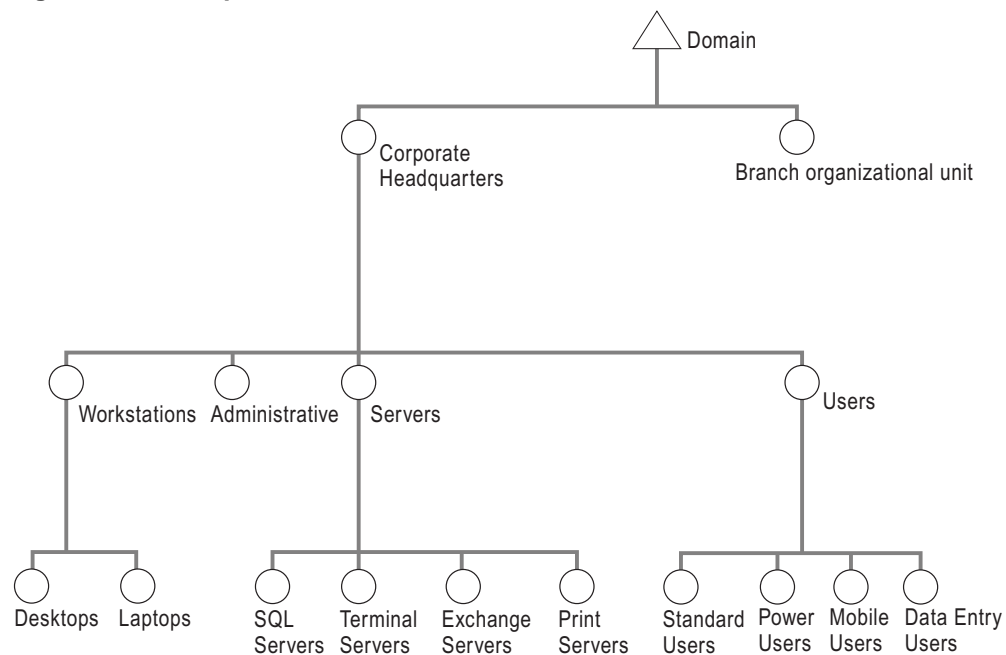
Delegating administrative authority You can create OUs within a domain and delegate administrative control for specific OUs to particular users or groups. Your OU structure might be affected by requirements to delegate administrative authority. For more information about planning for delegation of Active Directory administrative authority, see “Designing the Active Directory Logical Structure” in *Designing and Deploying Directory and Security Services* of this kit.

Applying Group Policy An OU is the lowest-level Active Directory container to which you can assign Group Policy settings.

Think primarily about the objects you want to manage when you approach the design of an OU structure. You might want to create a structure that has OUs organized by workstations, servers, and users near the top level. Depending on your administrative model, you might consider geographically based OUs either as children or parents of the other OUs, and then duplicate the structure for each location to avoid replicating across different sites. Add OUs below these only if doing so makes the application of Group Policy clearer, or if you need to delegate administration below these levels.

By using a structure in which OUs contain homogeneous objects, such as either user or computer objects but not both, you can easily disable those sections of a GPO that do not apply to a particular type of object. This approach to OU design, illustrated in Figure 2.3, reduces complexity and improves the speed at which Group Policy is applied. Keep in mind that GPOs linked to the higher layers of the OU structure are inherited by default, which reduces the need to duplicate GPOs or to link a GPO to multiple containers.

Note that the default Users and Computers containers cannot have Group Policy applied to them until you use the new Redirusr.exe and Redircomp.exe tools. When designing your Active Directory structure, the most important considerations are ease of administration and delegation.

Figure 2.3 Example OU Structure

Applying Group Policy to New User and Computer Accounts

New user and computer accounts are created in the CN=Users and CN=Computers containers by default. It is not possible to apply Group Policy directly to these containers, although they inherit GPOs linked to the domain. Redirusr.exe (for user accounts) and Redircomp.exe (for computer accounts) are two new tools included with Windows Server 2003 that enable you to change the default location where new user and computer accounts are created so you can more easily scope GPOs directly to newly created user and computer objects. These tools are located in %windir%\system32. By running Redirusr.exe and Redircomp.exe once for each domain, the domain administrator can specify the OUs into which all new user and computer accounts are placed at the time of creation. This allows administrators to manage these unassigned accounts by using Group Policy before the administrators assign them to the OU in which they are finally placed. You might want to consider restricting the OUs used for new user and computer accounts by using Group Policy to increase security around these accounts.

For more information about redirecting users and computers, see article 324949, “Redirecting the Users and Computers Containers in Windows Server 2003 Domains,” in the Microsoft Knowledge Base. To find this article, see the Microsoft Knowledge Base link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

For more information about the `redirusr.exe` and `redircomp.exe` tools, see the Redirecting Users and Computers link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Sites and Replication Considerations

As you determine which policy settings are appropriate, be aware of the physical aspects of Active Directory, which include the geographical location of sites, the physical placement of domain controllers, and the speed of replication.

GPOs are stored in both Active Directory and in the Sysvol folder on each domain controller. These locations have different replication mechanisms. Use the Resource Kit tool `Gpoutil.exe` to help diagnose problems when you suspect that a GPO might not have replicated across domain controllers. For more information about `Gpoutil.exe`, in Help and Support Center for Windows Server 2003, click **Tools**, and then click **Windows Resource Kit Tools Help**.

Domain controller placement is an issue when slow links, typically to clients at remote sites, are involved. If the network link speeds between a client and the authenticating domain controller fall below the default slow-link threshold of 500 kilobits per second, only the administrative template (registry-based) settings, the new Wireless Policy extension, and security settings are applied by default. All other Group Policy settings, including software distribution and folder redirection, are not applied by default. You can, however, modify this behavior by using Group Policy.

You can change the slow link threshold by using the **Group Policy Slow Link Detection** policy for both the user and computer aspects of a GPO. If necessary, you can also adjust which Group Policy extensions are processed below the slow-link threshold. However, it might be more appropriate to place a local domain controller at a remote location to serve your management needs.

Complying with Service Level Agreements

Some IT groups use service level agreements to specify how services should operate. For example, a service-level agreement might stipulate the maximum length of time required for computer startup and logon, how long users can use the computer after they log on, and so on. Service-level agreements often set standards for service responsiveness. For example, a service level agreement might define the amount of time allowed for a user to receive a new software application or gain access to a previously disabled feature. Issues that can affect service responsiveness are the site and replication topology, the positioning of domain controllers, and the location of Group Policy administrators.

To reduce the amount of time required to process a GPO, consider using one of the following options:

- If a GPO contains only computer or user settings, disable the portion of the policy that does not apply. The destination computer does not scan the portions of a GPO that you disable, which reduces processing time.
- When possible, combine smaller GPOs to form a consolidated GPO. This reduces the number of GPOs that apply to a user or computer. Applying fewer GPOs to a user or computer can reduce startup or logon times and make it easier to troubleshoot the policy structure.
- The changes you make to GPOs are replicated to domain controllers and result in new downloads to client or destination computers. If you have large or complex GPOs that require frequent changes, consider creating a new GPO that contains only the sections that you update regularly. Test this approach to determine whether the benefits you get by minimizing the impact on the network and improving the destination computer's processing time outweigh the increased troubleshooting potential by making the GPO structure more complex.



Note

You should implement a Group Policy change control process and log any changes made to GPOs. This can help you troubleshoot and correct problems with Group Policy objects. Doing so also helps comply with service level agreements that require keeping logs.

Defining Your Group Policy Objectives

When you plan the deployment of Group Policy, identify your specific business requirements and how Group Policy can help achieve them. You can then determine the most appropriate policy settings and configuration options to meet your requirements.

The objectives for each Group Policy implementation vary depending on user location, job needs, computer experience, and corporate security requirements. For example, in some cases, you might remove functionality from users' computers to prevent them from modifying system configuration files (which might disrupt computer performance), or you might remove applications that are not essential for users to perform their jobs. In other cases, you might use Group Policy to configure operating system options, specify Internet Explorer maintenance settings, or establish a security policy.

Having a clear understanding of your current organizational environment and requirements helps you design a plan that best meets your organization's requirements. Collecting information about the types of users (such as process workers and data entry workers) and existing and planned computer configurations is essential. Based on this information, you can define your Group Policy objectives.

Evaluating Existing Corporate Practices

To help you identify the appropriate Group Policy settings to use, begin by evaluating current practices in your corporate environment, including such things as:

- User requirements for various types of users.
- Current IT roles, such as the various administrative duties divided amongst administrator groups.
- Existing corporate security policies.
- Other security requirements for your server and client computers.
- Software distribution model.
- Network configuration.
- Data storage locations and procedures.
- Current management of users and computers.

Defining Group Policy Objectives

Next, as part of defining the goals for Group Policy, determine the following:

- Purpose of each GPO
- Owner of each GPO – the person who requested the policy and who is responsible for it
- Number of GPOs to use
- Appropriate container to link each GPO (site, domain, or OU)
- Types of policy settings contained in each GPO, and the appropriate policy settings for users and computers
- When to set exceptions to the default processing order for Group Policy
- When to set filtering options for Group Policy
- The software applications to install and their locations
- What network shares to use for redirecting folders
- The location of logon, logoff, startup, and shutdown scripts to execute

Establishing Group Policy Operational Guidelines

As you design and implement your Group Policy solution, it is also important to plan for the ongoing administration of Group Policy.

Establishing administrative procedures to track and manage GPOs can ensure that all changes are implemented in a prescribed manner.

To simplify and regulate ongoing management of Group Policy, it is recommended that administrators:

- Always stage Group Policy deployments using the following pre-deployment process:
 1. Use Group Policy Modeling to understand how a new GPO will interoperate with existing GPOs.
 2. Deploy new GPOs in a test environment modeled after your production environment.
 3. Use Group Policy Results to understand which GPO settings actually are applied in your test environment.
- Use GPMC to make backups of your GPOs on a regular basis.
- Use GPMC to manage Group Policy across the organization.
- Do not modify the default domain policy or default domain controller policy unless necessary. Instead, create a new GPO at the domain level and set it to override the default settings in the default policies.

- Define a meaningful naming convention for GPOs that clearly identifies the purpose of each GPO.
- Designate only one administrator per GPO. This prevents one administrator's work from being overwritten by another's.

Windows Server 2003 and GPMC allow you to delegate permission to edit and link GPOs to different groups of administrators. Without adequate GPO control procedures in place, delegated administrators can duplicate GPO settings, or create GPOs that conflict with settings set by another administrator or that are not in accordance with corporate standards. Such conflicts might adversely affect the users' desktop environment, generate increased support calls, and make troubleshooting GPOs more difficult.

Identifying Interoperability Issues

You need to consider possible interoperability issues when planning a Group Policy implementation in a mixed environment. Group Policy only applies to computers running Windows 2000, Windows XP Professional, or Windows Server 2003. You can only use GPMC on a computer running Windows XP Professional or Windows Server 2003 in an Active Directory network.

Windows Server 2003 and Windows XP Professional include many new Group Policy settings that are not used on Windows 2000. However, even if the client and server computers in your organization mostly run Windows 2000, and you have any Windows Server 2003 – based computers, you should use the Windows Server 2003 administrative templates (.adm files) because they are the latest .adm files and so are the most inclusive. If you apply a GPO with newer settings to a previous operating system that does not support the setting, it will not cause a problem. Destination computers that are running Windows 2000 or Windows XP Professional will simply ignore settings supported only in Windows Server 2003. To determine which settings apply to which operating systems, in the description for the setting, see the **Supported on** information, which explains which operating systems can read the setting.

If you are planning to deploy Group Policy in mixed environments, take the following Group Policy processing behavior into account.

- If the destination computer is running Microsoft® Windows NT® version 4.0, Microsoft Windows® 95, or Microsoft Windows® 98, it uses System Policy rather than Group Policy. System Policy is a Windows NT 4.0-style policy based on registry settings specified by using the System Policy Editor, Poledit.exe.
- If the destination computer is running Windows 2000, Windows XP Professional, or Windows Server 2003, and the computer account and the account for the logged-on user are both located in a Windows 2000 or Windows Server 2003 domain, both the computer and the user portions of a GPO are processed. If either the logged-on user account or the computer account is located in a Windows NT 4.0 domain, System Policy is processed for those accounts located in the domain.

Identifying and troubleshooting problems in a mixed environment where both System Policy and Group Policy apply can be difficult and time-consuming. When possible, move both the computer and the user account into a Windows 2000 or Windows Server 2003 domain. For more information about migrating user and computer accounts from a Windows NT 4.0 domain to Windows 2000 or Windows Server 2003 domain, see “Upgrading Windows NT 4.0 Domains to Windows Server 2003 Active Directory” in *Designing and Deploying Directory and Security Services* of this kit.

Determining When Group Policy Changes are Applied

Changes to Group Policy settings might not be immediately available on users’ desktops because changes to the Group Policy object must first replicate to the appropriate domain controller. In addition, clients use a 90-minute refresh period (randomized by up to approximately 30 minutes) for the retrieval of Group Policy. Therefore, it is rare for a changed Group Policy setting to apply immediately. Components of a GPO are stored in both Active Directory and on the Sysvol folder of domain controllers. Replication of a GPO to other domain controllers occurs by two independent mechanisms:

- Replication in Active Directory is controlled by Active Directory’s built-in replication system. By default, this typically takes less than a minute between domain controllers within the same site, if these domain controllers are part of a fresh-installed (not upgraded) forest running on Windows Server 2003–based domain controllers, or if the upgraded forest’s Functional Level is set to Windows Server 2003. However, in environments such as a partially upgraded forest that contains domain controllers running Windows 2000 and Windows Server 2003, a typical replication might take up to 15 minutes. This process can be even slower if your network is slower than a LAN.
- Replication of the Sysvol folder is controlled by the File Replication service (FRS). Within sites, replication occurs every 15 minutes. If the domain controllers are in different sites, the replication process occurs at set intervals based on site topology and schedule; the lowest interval is 15 minutes. In a Windows Server 2003 LAN environment, replication typically takes less than a minute.



Note

If it is critical to immediately apply a change to a specific group of users or computers in a specific site, you can connect to the domain controller closest to these objects, and then make the configuration change on that domain controller so those users get the updated policy first.

Policy Refresh Interval

The primary mechanisms for refreshing Group Policy are startup and logon. Group Policy is also refreshed on a regular basis. The policy refresh interval affects how quickly changes to Group Policy objects are applied. By default, clients and servers running Windows 2000, clients running Windows XP Professional, and destination servers running Windows Server 2003 check for changes to Group Policy objects every 90 minutes by using a randomized offset of up to 30 minutes. Domain controllers running Windows 2000 Server or Windows Server 2003 check for computer policy changes every five minutes. Although this polling frequency can be changed (by using one of these policy settings: **Group Policy Refresh Interval for Computers**, **Group Policy Refresh Interval for Domain Controllers**, or **Group Policy refresh Interval for Users**), shortening the frequency between refreshes is not recommended because of the potential increase in network traffic and the additional load placed on the domain controllers.

Triggering a Group Policy Refresh

If necessary, you can trigger a policy refresh manually from a local computer without waiting for the automatic background refresh. To do this, you can type `gpupdate` at the command line to refresh the user or computer policy settings. You cannot trigger a policy refresh by using GPMC.

The `gpupdate` command triggers a background policy refresh on the local computer from which the command is run. The `gpupdate` command is used in Windows Server 2003 and Windows XP environments. In Windows 2000, use the `secedit /refreshpolicy` command.

For more information about the `gpupdate` command, see “Changing the Group Policy Refresh Interval” later in this chapter.



Note

Some policy settings, such as folder redirection and the assignment of software applications, require the user to log off and log on again before they take effect. Software applications assigned to computers are installed only when the computer is restarted. See Help and Support Center for Windows Server 2003 for specific settings for information about when those settings take effect.

Identifying Issues Pertaining to Software Installation

Although Group Policy can successfully install software applications – especially in small- or medium-sized organizations – you need to determine if it is the best solution for your needs. Using Group Policy, assigned applications are installed or updated only when the computer is restarted or when the user logs on.

Using SMS for software deployment provides enterprise-level functionality that is not available with Group Policy-based software deployment, such as inventory-based targeting, status reporting, and scheduling. For this reason, you might use Group Policy to configure the desktop, set system security and access permissions, and use SMS to deliver software applications. This approach provides bandwidth control by scheduling application installation outside core business hours.

Your choice of tools depends on your requirements, your environment, and whether or not you need the additional functionality and security that SMS provides.

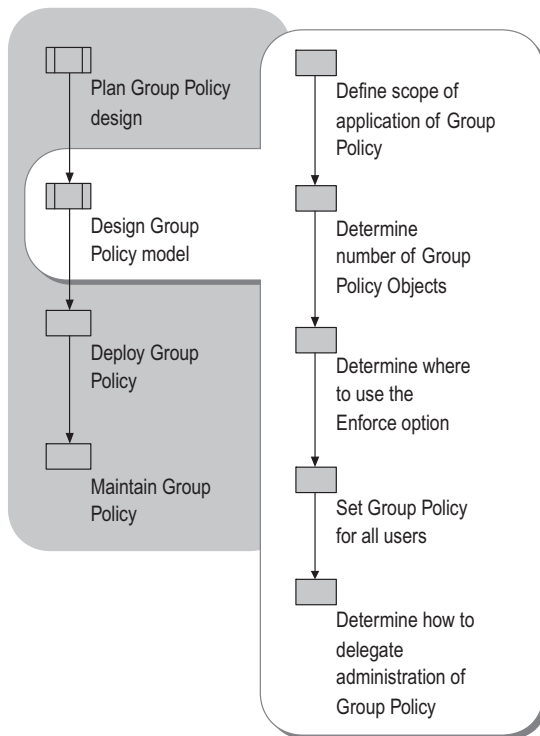
For more information about the Software Installation extension of Group Policy, see “Deploying a Managed Software Environment” in this book.

Designing Your Group Policy Model

Your primary objective is to design the GPO structure based on your business requirements. Keeping in mind the computers and users in your organization, determine which policy settings must be enforced across the organization, as well as which policy settings are applicable to all users or computers. Also determine which settings to use to configure computers or users according to type, function, or job role. Then group these different types of policy settings into GPOs and link them to the appropriate Active Directory containers.

Also, keep in mind the Group Policy inheritance model and how precedence is determined. By default, options set in GPOs linked to higher levels of Active Directory containers —sites, domains and OUs— are inherited by all containers at lower levels. However, inherited policy can be overridden by a GPO that is linked at a lower level. For example, you might use a GPO linked at a high level for assigning standard desktop wallpaper, but want a certain OU to get different wallpaper. To do so, you can link a second GPO to that specific lower-level OU. Because lower-level GPOs apply last, the second GPO will override the domain-level GPO and provide that specific lower-level OU with a different set of Group Policy settings. However, you can modify this default inheritance behavior by using **Block Inheritance** and **Enforced**.

Figure 2.4 illustrates the steps detailed in this section.

Figure 2.4 Group Policy Design Model

The following guidelines can help tailor your Group Policy design to the needs of your organization:

- Determine if there are any policy settings that must always be enforced for particular groups of users or computers. Create GPOs that contain these settings, link them to the appropriate site, domain, or OU, and designate these links as **Enforced** (formerly known as **No Override**). By setting this option, you enforce a higher-level GPO's settings by preventing GPOs in lower-level Active Directory containers from overriding them. For example, if you define a specific GPO at the domain level and specify that it is enforced, the policies that the GPO contains apply to all OUs under that domain; GPOs linked to the lower-level OUs cannot override that domain Group Policy.



Note

Use the **Enforced** and **Block Policy Inheritance** features sparingly. Routine use of these features can make it difficult to troubleshoot policy because it is not immediately clear to administrators of other GPOs why certain settings do or do not apply.

- Decide which policy settings are applicable to the entire organization and consider linking these to the domain. You can also use GPMC to copy GPOs or import GPO settings, thereby creating identical GPOs in different domains.
- Link the GPOs to the OU structure (or site), and then use Security Groups to selectively apply these GPOs to particular users or computers.
- Classify the types of computers and the roles or job function of users in your organization, group them into OUs, create GPOs to configure the environment for each as needed, and then link the GPOs to those OUs.
- Prepare a staging environment to test your Group Policy-based management strategy before deploying GPOs into your production environment. Think of this phase as staging your deployment. This is a crucial step toward ensuring that your Group Policy deployment will meet your management goals. This process is fully detailed in “Staging Group Policy Deployments,” in this book.

Defining the Scope of Application of Group Policy

To define the scope of application of Group Policy objects, consider these three main questions:

- Where will your GPOs be linked?
- What security filtering on the GPOs will you use?
- What WMI filters will be applied?

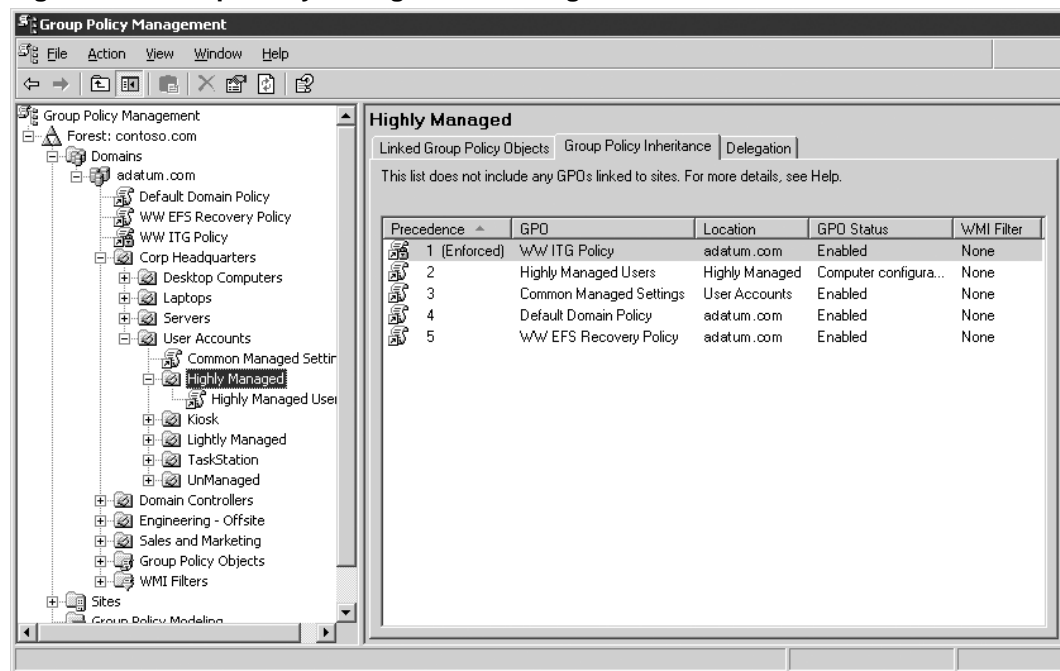
Also, remember that by default, Group Policy objects are inherited, cumulative, and affect all computers and users in an Active Directory container and its children. They are processed in the following order: local GPO (LGPO), site, domain, and then OU, with the last processed overriding the earlier GPOs. The default inheritance method is to evaluate Group Policy starting with the Active Directory container farthest from the computer or user object. The Active Directory container closest to the computer or user overrides Group Policy set in a higher-level Active Directory container unless you set the **Enforced (No Override)** option for that GPO link or if the **Block Policy inheritance** setting has been applied to the domain or OU. The LGPO is processed first, so settings from GPOs linked to Active Directory containers override the local settings. For more information about LGPOs, see the *Distributed Services Guide* of the *Windows Server 2003 Resource Kit* (or see the *Distributed Services Guide* on the Web at <http://www.microsoft.com/reskit>).

Another issue is that although you can link more than one GPO to an Active Directory container, you need to be aware of the processing order (priority). The GPO link with the lowest link order in the **Group Policy Object Links** list (displayed in the **Linked Group Policy Objects** tab in GPMC) has precedence by default. However, if one or more GPO links have the **Enforced** option set, the highest GPO link set to **Enforced** takes precedence.

Stated briefly, **Enforced** is a link property, **Block Policy Inheritance** is a container property, and **Enforced** takes precedence over **Block Policy Inheritance**. In addition, you can disable settings on the GPO itself in four other ways: A GPO can be disabled; and a GPO can have its computer settings disabled, its user settings disabled, or all of its settings disabled.

GPMC greatly simplifies these tasks by allowing you to view GPO inheritance across your organization and manage links from one MMC console. Figure 2.5 shows Group Policy inheritance as displayed in GPMC.

Figure 2.5 Group Policy Management Linking and Inheritance



Note

To view full details of inheritance and precedence for GPO links to a domain, site, or OU, you must have Read permissions on the domain, site, or OU containing the GPO links as well as on the GPOs. If you have Read access to the domain, site, or OU, but not on one of the GPOs linked there, it will appear as **Inaccessible GPO**, and you will not be able to read the name or other information for that GPO.

Determining the Number of Group Policy Objects

The number of Group Policy objects you need depends on your approach to design, the complexity of the environment, your objectives, and the scope of the project. If you have a multi-domain forest, or multiple forests, you might find that the number of GPOs required in each domain is different. Domains supporting highly complex business environments with a diverse user population typically require more GPOs than smaller, simpler domains.

As the number of GPOs required to support an organization increases, so can the workload of Group Policy administrators. There are steps you can take to ease the administration of Group Policy. In general, you should group settings that apply to a given set of users or computers and are managed by a common set of administrators into a single GPO. Further, if various groups of users or computers have common requirements, and only a few of the groups need incremental changes, consider applying the common requirements to all these groups of users or computers by using a single GPO linked high in the Active Directory structure, and then add additional GPOs, which apply only the incremental changes, at the relevant OU. This might not always be possible or practical, so you might need to make exceptions to this guideline. If so, be sure to keep track of them. Note that a maximum of 999 GPOs is supported for processing GPOs on any one user or computer. If you exceed the maximum, no GPOs will be processed. This limitation affects only the number of GPOs that can be applied at the same time; it does not affect the number of GPOs you can create and store in a domain.

Consider that the number of GPOs applied to a computer affects startup time, and the number of GPOs applied to a user affects the amount of time needed to log on to the network. The greater the number of Group Policy objects that are linked to a user — especially the greater the number of settings within those GPOs — the longer it takes to process them whenever a user logs on. During the logon process, each GPO from the user's site, domain, and OU hierarchy is applied, provided both the Read and Apply Group Policy permissions are set for the user. In GPMC, the Read and Apply Group Policy permissions are managed as a single unit called Security Filtering.

If you use Security Filtering and you remove the Apply Group Policy permission for a given user or group, also remove the Read permission, unless you need that user to have read access for some reason. (If you are using GPMC, you need not worry about this, because GPMC does this for you automatically.) If the Apply Group Policy permission is not set, but the Read permission is, the GPO is still inspected (although not applied) by any user or computer that is in the OU hierarchy where the GPO is linked. This inspection process increases logon time slightly.

Always test your Group Policy solution in a test environment to ensure that the policy settings you define do not unacceptably prolong the time it takes to display the logon screen, and that they comply with desktop service level agreements. During this staging period, log on with a test account to gauge the net effect of several GPOs on objects in your environment.

Linking GPOs

To apply the settings of a GPO to the users and computers of a domain, site, or OU, you need to add a link to that GPO. You can add one or more GPO links to each domain, site, or OU by using GPMC. Keep in mind that creating and linking GPOs is a sensitive privilege that should be delegated only to administrators who are trusted and understand Group Policy.

Linking GPOs to the Site

If you have a number of policy settings to apply to computers in a particular physical location only — certain network or proxy configuration settings, for example — these settings might be appropriate for inclusion in a site-based policy. Because domains and sites are independent, it is possible that computers in the site might need to cross domains to link the GPO to the site. In this case, make sure there is good connectivity.

If, however, the settings do not clearly correspond to computers in a single site, it is better to assign the GPO to the domain or OU structure rather than to the site.

Linking GPOs to the Domain

Link GPOs to the domain if you want them to apply to all users and computers in the domain. For example, security administrators often implement domain-based GPOs to enforce corporate standards. They might want to create these GPOs with the GPMC **Enforce** option enabled to guarantee that no other administrator can override these settings.



Important

If you need to modify some of the settings contained in the **Default Domain Policy GPO**, it is recommended that you create a new GPO for this purpose, link it to the domain, and set the **Enforce** option. In general, do not modify this or the **Default Domain Controller Policy GPO**. If you do, be sure to back up these and any other GPOs in your network by using GPMC to ensure you can restore them.

As the name suggests, the **Default Domain Policy GPO** is also linked to the domain. The **Default Domain Policy GPO** is created when the first domain controller in the domain is installed and the administrator logs on for the first time. This GPO contains the domain-wide account policy settings, Password Policy, Account Lockout Policy, and Kerberos Policy, which is enforced by the domain controller computers in the domain. All domain controllers retrieve the values of these account policy settings from the **Default Domain Policy GPO**. In order to apply account policies to domain accounts, these policy settings must be deployed in a GPO linked to the domain, and it is recommended that you set these settings in the Default Domain Policy. If you set account policies at a lower level, such as an OU, the settings only affect local accounts (non-domain accounts) on computers in that OU and its children.

Before making any changes to the default GPOs, be sure to back up the GPO using GPMC. If for some reason there is a problem with the changes to the default GPOs and you cannot revert back to the previous or initial states, you can use the Dcgpofix.exe tool to recreate the default policies in their initial state.

Dcgpofix.exe is a command-line tool that completely restores the Default Domain Policy GPO and Default Domain Controller GPO to their original states in the event of a disaster where you cannot use GPMC. Dcgpofix.exe restores only the policy settings that are contained in the default GPOs at the time they are generated. The only Group Policy extensions that include policy settings in the default GPOs are RIS, Security, and EFS. Dcgpofix.exe does not restore other GPOs that administrators create; it is only intended for disaster recovery of the default GPOs.

Note that Dcgpofix.exe does not save any information created through applications, such as SMS or Exchange. The Dcgpofix.exe tool is included with Windows Server 2003 and only works in a Windows Server 2003 domain.

Dcgpofix.exe is located in the C:\Windows\Repair folder. The syntax for Dcgpofix.exe is as follows:

```
DCGPoFix [/Target: Domain | DC | BOTH]
```

Table 2.1 describes the options you can use with the command line parameter /Target: when using the Dcgpofix.exe tool.

Table 2.1 Dcgpofix.exe Options for Using the /Target Parameter

/Target option:	Description of option
DOMAIN	Specifies that the Default Domain Policy should be recreated.
DC	Specifies that the Default Domain Controllers Policy should be recreated.
BOTH	Specifies that both the Default Domain Policy and the Default Domain Controllers Policy should be recreated.

For more information about Dcgpofix.exe, in Help and Support Center for Windows Server 2003 click **Tools**, and then click Command-line reference A-Z.

Linking GPOs to the OU Structure

Most GPOs are normally linked to the OU structure because this provides the most flexibility and manageability:

- You can move users and computers into and out of OUs.
- OUs can be rearranged if necessary.
- You can work with smaller groups of users who have common administrative requirements.
- You can organize users and computers based on which administrators manage them.

Organizing GPOs into user- and computer-oriented GPOs can help make your Group Policy environment easier to understand and can simplify troubleshooting. However, separating the user and computer components into separate GPOs might require more GPOs. You can compensate for this by adjusting the **GPO Status** to disable the user or computer configuration portions of the GPO that do not apply and to reduce the time required to apply a given GPO.

Changing the GPO Link Order

Within each domain, site, and OU, the link order controls the order in which GPOs are applied. To change the precedence of a link, you can change the link order, moving each link up or down in the list to the appropriate location. Links with the lowest number have higher precedence for a given site, domain, or OU. For example, if you add six GPO links and later decide that you want the last one that you added to have the highest precedence, you can adjust the link order of the GPO link so it has link order of 1. To change the link order for GPO links for a domain, OU, or site, use GPMC.

Using Security Filtering to Apply GPOs to Selected Groups

By default, a GPO affects all users and computers contained in the linked site, domain, or OU. However, you can use Security Filtering on a GPO to modify its effect to apply only to a specific user or the members of a security group by modifying the permissions on the GPO. By combining Security Filtering with appropriate placement in OUs, you can target any given set of users.

In order for a GPO to apply to a given user or computer, that user or computer must have both **Read** and **Apply Group Policy** permissions on the GPO. By default, Authenticated Users have both **Apply Group Policy** and **Read** permissions set to **Allow**. Both of these permissions are managed together as a single unit by using Security Filtering in GPMC.

To set the permissions for a given GPO, in the GPMC console tree, expand **Group Policy Objects** in the forest and domain containing that GPO. Click the GPO, and in the details pane, on the **Scope** tab, under **Security Filtering**, remove **Authenticated Users**, and then click **Add** to add a new group.

To filter a GPO by a particular security group, add that group to the Security Filtering section on the **Scope** tab of a GPO in GPMC.

For example, if you want only a subset of users within an OU to receive a GPO, remove the Authenticated Users from Security Filtering. Instead, add a new group with Security Filtering permissions that contains the subset of users who are to receive the GPO. Only members of this group that are within the site, domain, or OU where the GPO is linked receive the GPO; members of the group in other sites, domains, or OUs do not receive the GPO.

You might want to prevent certain Group Policy settings from applying to the Administrator group. To accomplish this, you can do one of the following:

- Create a separate OU for administrators and keep this OU out of the hierarchy to which you apply most of your management. In this way administrators do not receive most of the settings that you provide for managed users. If this separate OU is a direct child of the domain, the only possible settings administrators receive are settings from GPOs linked either to the domain or the site. Typically, only generic, broadly applicable settings are linked here, so it might be acceptable to have administrators receive these settings. If this is not what you intend, you can set the **Block Inheritance** option on the administrators' OU.

- Have administrators use separate administrative accounts for use only when they perform administrative tasks. When not performing administrative tasks, they would still be managed.
- Use Security Filtering in GPMC so that only non-administrators will receive the settings.

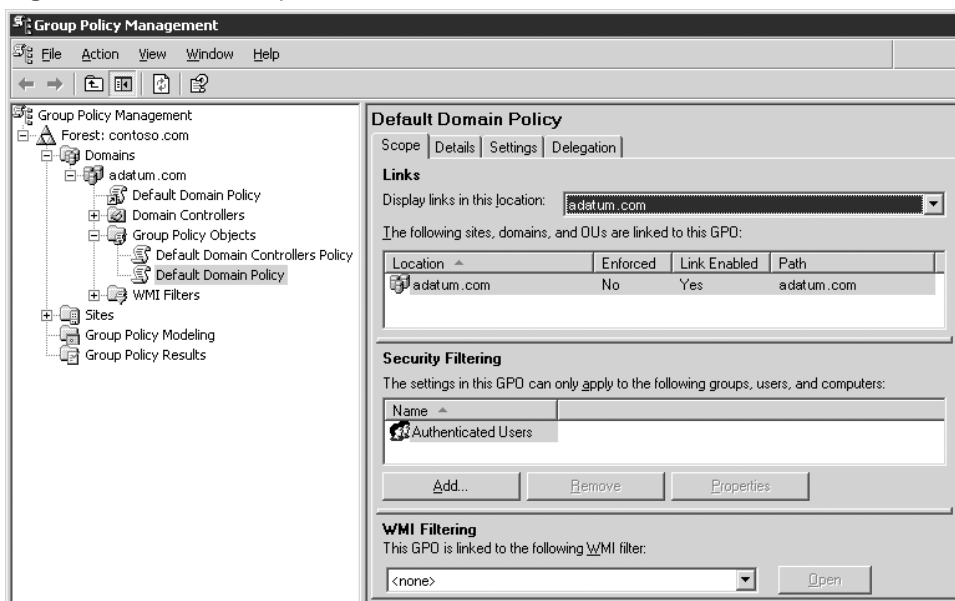
Applying WMI Filters

You can use WMI filters to control the application of GPOs. Each GPO can be linked to one WMI filter, however, the same WMI filter can be linked to multiple GPOs. Before you can link a WMI filter to a GPO, you must create the filter. The WMI filter is evaluated on the destination computer (running either Windows XP or Windows Server 2003) during processing of Group Policy. The GPO will only apply if the WMI filter evaluates to TRUE. On Windows 2000–based computers, the WMI filter is ignored and the GPO is always applied.

Using GPMC, you can perform the following operations for WMI filters: create and delete, link and unlink, copy and paste, import and export, and view and edit attributes.

WMI filters can only be used if at least one domain controller in the domain is running Windows Server 2003, or if you have run ADPrep with the /Domainprep option in that domain. If not, the **WMI Filtering** section on the **Scope** tab for GPOs and the **WMI Filters** container under the domain will not be present. See Figure 2.6 to help you identify the items discussed in this section.

Figure 2.6 GPMC Scope Tab



Setting WMI Filtering Options

WMI exposes management data from a destination computer, such as hardware and software inventory, settings, and configuration information, including data from the registry, drivers, the file system, Active Directory, SNMP, Windows Installer, and networking. Administrators can create WMI filters, which consist of one or more queries based on this data — to control whether the GPO is applied. The filter is evaluated on the destination computer (which must be running either Windows XP Professional or Windows Server 2003). If the WMI filter evaluates to true, the GPO is applied to that destination computer; if the filter evaluates to false, the GPO is not applied. On Windows 2000–based client or server targets, WMI filters are ignored, and the GPO is always applied. In the absence of any WMI Filter, the GPO is always applied.

Administrators can use WMI filters to target Group Policy based on a variety of objects and other parameters. Table 2.2 illustrates example query criteria that might be specified for WMI filters.

Table 2.2 Sample WMI Filters

WMI Data Queried	Sample Query Criteria
Services	Computers with the DHCP service running
Registry	Computers that have a specified registry key or entry populated
Windows Event Log	Computers that reported an audit event in the last five minutes
Operating system version	Computers running Windows Server 2003 and later
Hardware inventory	Computers with a Pentium III processor
Hardware configuration	Computers with network adapters on in level 3
Service associations	Computers that have any service dependent on SNA service
Ping	Computers that can ping Server1 in less than 100 milliseconds

A WMI filter consists of one or more WMI Query Language (WQL) queries. The WMI filter applies to every setting in the GPO, so administrators must create separate GPOs if they have different filtering requirements for different settings. The WMI filters are evaluated on the destination computer after the list of potential GPOs is determined and filtered based on security group membership. For detailed information about WMI filters, see the *Distributed Services Guide* of the *Windows Server 2003 Resource Kit* (or see the *Distributed Services Guide* on the Web at <http://www.microsoft.com/reskit>).

Although you can do limited inventory-based targeting for software deployment by combining Group Policy-based software deployment with WMI filters, this is not recommended as a general practice for the following reasons:

- Each GPO can only have one WMI Filter. If applications have different inventory requirements, you need multiple WMI filters and therefore multiple GPOs. Increasing the number of GPOs impacts startup and logon times and also increases management overhead.
- WMI filters can take significant time to evaluate, so they can slow down logon and startup time. The amount of time depends on the construction of the query.



Note

It is recommended that you use WMI filters primarily for exception management. They can be powerful solutions for targeting GPOs to specific users and computers, but because WMI filters are evaluated every time Group Policy is processed, they increase startup and logon time. Also, there is no time-out for WMI filters. Use them only when necessary.

Example WMI Filters

WMI filters are most useful as tools for exception management. By filtering for particular criteria, you can target particular GPOs to only specific users and computers. The following are WMI filters that illustrate this technique.

Targeting Based on Operating System

In this example, an administrator wants to deploy an enterprise monitoring policy, but wants to target only Windows XP Professional-based computers. The administrator can create a WMI filter such as the following:

```
Select * from Win32_OperatingSystem where Caption = "Microsoft Windows XP Professional"
```

Most WMI filters use the **Root\CimV2** namespace, and this option is populated by default in the GPMC user interface.

Because WMI filters are ignored on Windows 2000-based computers, a filtered GPO will always be applied on them. However, you can work around this by using two GPOs and giving the one with Windows 2000 settings higher precedence (using link order). Then use a WMI filter for that Windows 2000 GPO, and only apply it if the operating system is Windows 2000, not Windows XP Professional. The Windows 2000-based computer will receive the Windows 2000 GPO and will override the settings in the Windows XP Professional GPO. The Windows XP Professional client will receive all the settings in the Windows XP Professional GPO.

Targeting Based on Hardware Inventory

In this example, an administrator wants to distribute a new network connection manager tool only to desktops that have modems. The administrator can deploy the package by using the following WMI filter to target those desktops:

```
Select * from Win32_POTSModem Where Name = "MyModem"
```

If you use Group Policy with a WMI filter, remember that the WMI filter applies to all settings in the GPO. If you have different requirements for different deployments, you need to use different GPOs, each with its own WMI filter.

Targeting Based on Configuration

In this example, an administrator does not want to apply a GPO on computers that have multicasting turned on. The administrator can use the following filter to identify those computers which have multicast support:

```
Select * from Win32_NetworkProtocol where SupportsMulticasting = true
```

Targeting Based on Amount of Disk Space and File System Type

In this example, an administrator wants to target computers that have more than 10 megabytes (MB) of available space on the C, D, or E partition. The partitions must be located on one or more local fixed disks and they must be running the NTFS file system. The administrator can use the following filter to identify computers that meet these criteria:

```
SELECT * FROM Win32_LogicalDisk WHERE (Name = "C:" OR Name = "D:" OR Name = "E:")
AND DriveType = 3 AND FreeSpace > 10485760 AND FileSystem = "NTFS"
```

In the preceding example, DriveType value = 3 represents a local disk and FreeSpace units are in Bytes (10 MB = 10,485,760 Bytes).

► To Create a WMI Filter

1. In the GPMC console tree, right-click **WMI Filters** in the forest and domain in which you want to add a WMI filter.
2. Click **New**.
3. In the **New WMI Filter** dialog box, type a name for the new WMI Filter in the **Name** box, and then type a description of the filter in the **Description** box.
4. Click **Add**.
5. In the **WMI Query** dialog box, either leave the default namespace (root\CIMv2) or enter another namespace by doing one of the following:
 - In the **Namespace** box, type the name of the namespace that you want to use for the WMI query. The default is **Root\CimV2**. In most cases, you do not need to change this.
 - Click **Browse**, select a namespace from the list, and then click **OK**.
6. Type a WMI query in the **Query** box, and then click **OK**.
7. To add more queries, repeat steps 4 through 6 to add each query.
8. After you add all the queries, click **Save**.

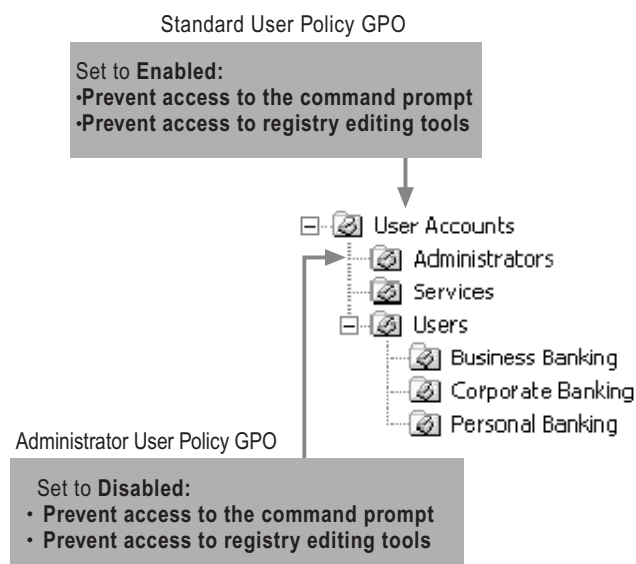
The WMI filter is now available to be linked.

Using Group Policy Inheritance

It is often useful to define a corporate-standard GPO. As used here, *corporate standard* refers to policy settings that apply to a broad set of users in an organization. An example of where defining a corporate standard GPO might be appropriate is a business requirement that states: “Only specially authorized users can access the command prompt or the registry editor.” Group Policy inheritance can help you apply these corporate standards while customizing settings for different groups of users.

One way to do this is to set the policy settings **Prevent access to the command prompt**, and **Prevent access to registry editing tools** in a GPO, such as the Standard User Policy GPO that is linked to an OU, such as the User Accounts OU. By default this will apply these settings to all users in that OU. Then create a GPO, such as an Administrator User Policy GPO, which explicitly allows administrators access to the command prompt and registry editing tools. Link the GPO to the Administrators OU, which overrides the settings configured in the Standard User Policy GPO. This approach is illustrated in Figure 2.7.

Figure 2.7 Standard User Policy GPO



If another group of users requires access to the command prompt, but not the registry, you can create another GPO that allows them to do so. Access to the registry editing tools is still denied because the new GPO does not override the registry tools setting made in the Standard User Policy GPO. Typically, a corporate standard GPO includes more settings and configuration options than those shown in the preceding illustration. For example, corporate standard Group Policy objects are typically used to achieve the following:

- Remove all potentially harmful and nonessential functionality for users.
- Define access permissions, security settings, and file system and registry permissions for member servers and workstations.

Typically, GPOs are assigned to the OU structure instead of the domain or site. If you structure your OU model around users, workstations, and servers, it is easier to identify and configure corporate standard settings. You can also disable either the user or computer portions of policy that do not apply, making Group Policy easier to manage.

When you set default values for security-related settings such as restricted group membership, file system access permissions, and registry access permissions, it is important to understand that these settings work on a last-writer-wins principle, and that the settings are not merged. The following example demonstrates this principle.

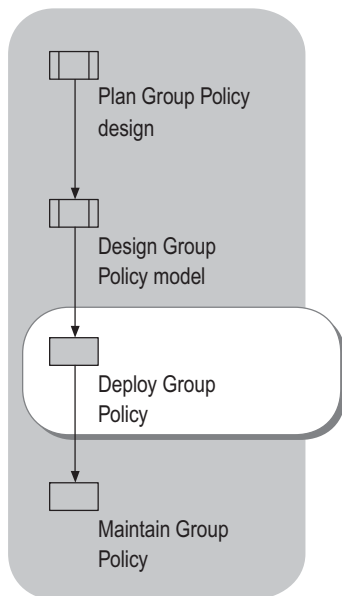
Example: Last-Writer-Wins Principle

An administrator creates a Default Workstations GPO that defines the membership of the local Power Users group as the Technical Support and Help Desk groups. The Business Banking group wants to add the Business Banking Support group to this list and creates a new Default Workstations GPO to do so. Unless the new GPO specifies that all three groups are members of Power Users, only the Business Banking Support group has Power User rights on affected workstations.

Deploying Group Policy

Before deploying your Group Policy solution, administrators need to be familiar with the procedures for working with GPOs, including creating GPOs, importing settings, backing up and restoring GPOs, editing and linking GPOs, setting exceptions to default inheritance of GPOs, filtering the application of GPOs, delegation of administration, and using Group Policy Modeling for planning and Group Policy Results for evaluating GPO application. Figure 2.8 illustrates the place of this step in the process of designing a Group Policy infrastructure.

Figure 2.8 Deploying Group Policy



Always fully test your GPOs in safe (nonproduction) environments prior to production deployment. The more you plan, design, and test GPOs prior to deployment, the easier it is to create, implement, and maintain an optimal Group Policy solution. The importance of testing and pilot deployments in this context cannot be overemphasized. Your tests should closely simulate your production environment.

A design is not complete until you test and validate all its significant variations and your deployment strategy. Thorough testing of your GPO implementation strategy is not possible until you configure your GPOs using specific settings, such as security settings, and desktop and data management. Do this for each group of users and computers in the network. Use your test environment to develop, test, and validate specific GPOs. Take full advantage of the GPMC Modeling Wizard and the Results Wizard.

Consider an iterative implementation of Group Policy. That is, rather than deploying 100 new Group Policy settings, stage and then initially deploy only a few settings to validate that the Group Policy infrastructure is working well.

For more information about this phase, see “Staging Group Policy Deployments” in this book. This chapter details the information you need to deploy Group Policy into your production environment, but never deploy an untested GPO. For step-by-step details about creating a new GPO, search Help and Support Center for Windows Server 2003 using the keywords “Group Policy Object Editor.” For step-by-step details about using GPMC to perform other GPO tasks such as importing settings from one GPO into another, see Help in GPMC.

Table 2.3 lists the six sample standard desktop configurations that are described in “Planning a Managed Environment” in this book. Examining these standard configurations can help you configure your Group Policy deployment. Each file is a GPO with sample standard desktop configurations you can copy into your test environment. The actual settings for each GPO are listed in the corresponding HTML reports.

Table 2.3 Sample Standard Desktop Configurations

Standard Desktop Configuration	Scenario File Name
Lightly managed desktop	LightlyManagedDesktop.htm
Mobile users desktop	MobileUser.htm
Multiuser desktop	MultiuserDesktop.htm
Highly managed desktop	Appstation.htm
TaskStation desktop	Taskstation.htm
Kiosk	Kiosk.htm

For information about using the sample GPOs, see the whitepaper at the Implementing Common Desktop Management Scenarios link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Creating and Working with GPOs

Because changes to a GPO take place immediately, keep the GPO unlinked from its production location (site, domain, or OU) until you have fully tested it in a test environment. While you are developing the GPO, keep it either unlinked or linked to a test OU.

For more information about testing your Group Policy configurations prior to deployment, see “Staging Group Policy Deployments” in this book. This section details the process of creating and deploying GPOs.

The following procedures detail creating GPOs by using GPMC:

► **To create an unlinked Group Policy object**

1. Expand the GPMC console tree until you see **Group Policy Objects** in the container domain for which you want to create a new GPO.
2. Right-click **Group Policy Objects**.
3. Click **New**.
4. In the **New GPO** dialog box, specify a name for the new GPO, and then click **OK**.

► **To edit a GPO**

1. In the GPMC console tree, right-click the GPO you want to edit, and then click **Edit**. This starts the Group Policy Object Editor MMC snap-in.
2. In the Group Policy Object Editor console tree, expand the items to view their policies in the details pane.
3. In the details pane, double-click the names of the settings to open their **Properties** dialog boxes and change their settings. Note that some settings, such as the settings for deploying a new software installation package, use unique user interfaces.

The primary mechanism for applying the settings in a GPO to users and computers is by linking the GPO to a container in Active Directory. GPOs can be linked to three types of containers in Active Directory: sites, domains, and organizational units. A GPO can be linked to multiple Active Directory containers.

► **To link a GPO**

GPOs are stored on a per-domain basis. For example, if you link a GPO to an OU, the GPO is not actually located in that OU. A GPO is a per domain object that can be linked anywhere in the forest. The UI in GPMC helps clarify the distinction between links and actual GPOs. In GPMC, you can link a GPO to Active Directory containers using any of the following methods:

- Right-click a site, domain, or OU item, and then click **Link an existing GPO here**. This option is equivalent to choosing **Add** on the **Group Policy** tab that was available in the Active Directory Users and Computers MMC snap-in, prior to installing GPMC. This requires that the GPO already exist in the domain.
- Drag a GPO from under the **Group Policy objects** item to the OU. This drag-and-drop functionality works only within the same domain.

You can also use the GPMC user interface to simultaneously create a new GPO and link it at the same time in one step, as described below.

► **To create and link a GPO**

- Right-click a domain or OU item, and then click **Create and Link a GPO here**. This option is equivalent to clicking **New** on the **Group Policy** tab that was available in the Active Directory Users and Computers snap-in, prior to installing GPMC. In the **New GPO** dialog box, type a name for the new GPO, and then click **OK**. Although this operation is presented in GPMC as one action to the user, there are actually two steps taking place. First, a GPO is created in the domain, and second, the new GPO is linked to the domain or OU.

To create a GPO and link it to a site, you must first create the GPO in the domain, and then link it.

► **To unlink a GPO from a site, domain, or OU**

1. In the GPMC console tree, right-click the GPO you want to unlink.
2. In the details pane, click the **Scope** tab.
3. In the **Links** section, right-click the Active Directory object.
4. Select **Delete Link** from the drop-down list.



Note

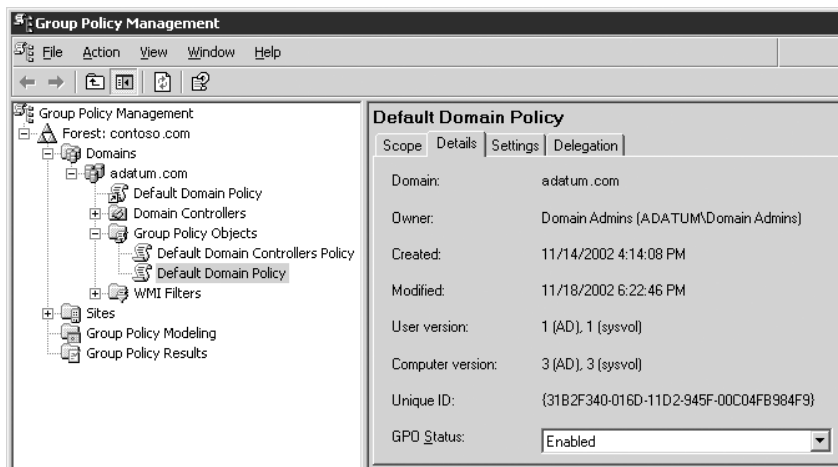
Deleting a link is different than deleting a GPO. If you delete only the link, the GPO still exists, as do any other existing links to that GPO. However, if you delete a GPO, you will be prompted to delete the GPO and all links to it in this domain. This does not delete links to the GPO from other domains. Be sure to remove links to the GPO in other domains before deleting this GPO in this domain.

Disabling the User or Computer Configuration Property of a GPO

If you are creating a GPO to set only user-related policy settings, you can disable the Computer Configuration portion of the GPO. Doing this slightly reduces computer startup time because the Computer GPO does not have to be evaluated to determine if any policies exist. If you are configuring only computer-related policy settings, turn off the User Configuration portion of the GPO.

See Figure 2.9 to help you identify the GPMC items referred to in the procedure that follows.

Figure 2.9 Setting GPO Status



► **To disable the User or Computer Configuration settings in a GPO**

1. In the GPMC console tree, click the GPO you want to modify.
2. Click the **Details** tab, or right-click the GPO.
3. In the **GPO Status** drop-down box, select one of these choices:
 - **All settings disabled**
 - **Computer settings disabled**
 - **Enabled (default)**
 - **User settings disabled**

Special Considerations for Site-linked GPOs

GPOs linked to sites might be appropriate to use for setting policy for proxy settings and network-related settings. Any GPO that is linked to a site container is applied to all computers in that site, regardless of which domain in the forest the computer belongs to. This has the following implications:

- Ensure that the computers do not access a site Group Policy object across a WAN link, which would lead to significant performance issues.
- By default, to manage site GPOs, you need to be either an Enterprise Admin, or the domain admin of the forest root domain.

- Active Directory service data-replication between domain controllers in different sites occurs less frequently than replication between domain controllers in the same site, and occurs during scheduled periods only. Between sites, FRS replication occurs spontaneously, and is not determined by the site link replication schedule; this is not an issue within sites. The directory service replication schedule and frequency are properties of the site links that connect sites. The default inter-site replication frequency is three hours. To change it, go to the appropriate site link, go to the IP link, and change the replication frequency or schedule as needed.

Changing either the replication frequency or schedule can significantly affect policy. For example, assume that you have replication set to three hours or longer, and you create a GPO and link it to an OU in a domain that spans several sites. You will likely need to wait several hours before all users in that OU receive the GPO.

If most of the users in an OU are in a remote location, and you have a domain controller in that site, you can work around inter-site replication latency by performing all Group Policy operations on a domain controller in that site.

Using Loopback Processing to Configure User Settings

The **User Group Policy loopback processing mode** policy setting is an advanced option that is intended to keep the configuration of the computer the same regardless of who logs on. This option is appropriate in certain closely managed environments, such as servers, terminal servers, classrooms, public kiosks, and reception areas. Setting the loopback processing mode policy setting applies the same user settings for any user who logs onto the computer, based on the computer.

When you apply Group Policy objects to users, normally the same set of user policy settings applies to those users when they log on to any computer. By enabling the loopback processing policy setting in a GPO, you can configure user policy settings based on the computer that they log on to. Those settings are applied regardless of which user logs on. When you use this option, you must ensure that both the computer and user portions of the GPO are enabled.

You can set the loopback policy in the Group Policy Object Editor snap-in by using the **User Group Policy loopback processing mode** policy setting under **Computer Settings\Administrative settings\System\Group Policy**. Two options are available:

Merge mode In this mode, the list of GPOs for the user is gathered during the logon process. Then, the list of GPOs for the computer is gathered. Next, the list of GPOs for the computer is added to the end of the GPOs for the user. As a result, the computer's GPOs have higher precedence than the user's GPOs.

Replace mode In this mode, the list of GPOs for the user is not gathered. Instead, only the list of GPOs based on the computer object is used. The User Configuration settings from this list are applied to the user.

Delegating Administration of Group Policy

Your Group Policy design will probably call for delegating certain Group Policy administrative tasks. Determining to what degree to centralize or distribute administrative control of Group Policy is one of the most important factors to consider when assessing the needs of your organization. In organizations that use a centralized administration model, an IT group provides services, makes decisions, and sets standards for the entire company. In organizations that use a distributed administration model, each business unit manages its own IT group.

You can delegate the following Group Policy tasks:

- Creating GPOs
- Managing individual GPOs (for example, granting Edit or Read access to a GPO)
- Performing the following tasks on sites, domains, and OUs:
 - Managing Group Policy links for a given site, domain, or OU
 - Performing Group Policy Modeling analyses for objects in that container (not applicable for sites)
 - Reading Group Policy Results data for objects in that container (not applicable for sites)
- Creating WMI filters
- Managing and editing individual WMI filters

Based on your organization's administrative model, you need to determine which aspects of configuration management can best be handled at the site, domain, and OU levels. You also need to determine how responsibilities at each site, domain, and OU level might be further subdivided among the available administrators or administrative groups at each level.

When deciding whether to delegate authority at the site, domain, or OU level, remember the following points:

- Authority delegated at the domain level affects all objects in the domain, if the permission is set to inherit to all child containers.
- Authority delegated at the OU level can affect either that OU only, or that OU and its child OUs.
- Managing permissions is easier and more efficient if you assign control at the highest OU level possible.
- Authority delegated at the site level is likely to span domains and can influence objects in domains other than the domain where the GPO is located.

Following are descriptions of how to use GPMC to perform these delegation tasks.

Delegating management of individual GPOs

Using GPMC, you can easily grant additional users permissions on a GPO. GPMC manages permissions at the task level. There are five levels of allowed permissions on a GPO: Read, Edit, and Edit/Delete/Modify Security, Read (from Security Filtering), and Custom. These permission levels correspond to a fixed set of low-level permissions. Table 2.4 shows the corresponding low-level permissions for each option.

Table 2.4 GPO Permission Options and Low Level Permissions

GPO Permission Option	Low Level Permissions
Read	Allow Read Access on the GPO.
Read (from Security Filtering)	This setting cannot be set directly, but appears if the user has Read and Apply Group Policy permissions to the GPO, which is set using Security Filtering on the Scope tab of the GPO.
Edit settings	Allow Read, Write, Create Child Objects, Delete Child Objects.
Edit, delete, and modify security	Allow Read, Write, Create Child Objects, Delete Child Objects, Delete, Modify Permissions, and Modify Owner. This essentially grants full control on the GPO, except that the “Apply Group Policy” permission is not set.
Custom	Any other combinations of rights, such as denying permissions, appear as Custom permissions. You cannot set custom rights by clicking Add. They can only be set by using the ACL editor directly, which can be started by clicking the Advanced button.

You can click **Add** to grant users permissions on a GPO. This starts the object picker so you can find the desired user or group to set the permission level. You can then set the permission level by selecting the **Read**, **Edit**, or **Edit, Delete, Modify Security** permissions.

Note that the **Apply Group Policy** permission, which is used for Security Filtering, cannot be set using the **Delegation** tab. Because setting **Apply Group Policy** is used for scoping the GPO, this permission is managed on the **Scope** tab of the GPMC user interface. When you grant a user Security Filtering on the **Scope** tab, you are actually setting both the **Read** and **Apply Group Policy** permissions.

You can grant additional groups and users permissions on a GPO by using GPMC, as described above. Table 2.5 lists the default security permission settings for a GPO.

Table 2.5 Default Security Permissions for GPOs.

Security Group	Permissions
Authenticated Users	Read (from Security Filtering)
Enterprise Domain Controllers	Read
Domain Administrators Enterprise Administrators Creator Owner SYSTEM	Edit settings, delete, modify security



Note

Because Administrators are also part of the Authenticated Users group, they have the Apply Group Policy ACE set to Allow by default; as a result, policy settings apply to them as well if they are located in the container where the GPO is linked.

Delegating Group Policy-Related Tasks on Sites, Domains, and OUs

You can manage three Group Policy tasks on a per-container basis in Active Directory:

- Linking GPOs to an Active Directory container (site, domain, or OU)
- Performing Group Policy Modeling analysis for objects in that container (domains and OUs)
- Reading Group Policy Results data for objects in that container (domains and OUs)

By default, Domain Administrators have GPO linking permission for domains and OUs, and Enterprise Administrators and Domain Administrators of the forest root domain can manage links to sites. You can delegate permissions to additional groups and users by using GPMC.

By default, access to Group Policy Modeling and remote access to Group Policy Results data is restricted to Enterprise Administrators and Domain Administrators. Organizations can delegate access to these tasks to lower-level administrators by setting these permissions in GPMC.

The following procedures detail Group Policy delegation tasks on Active Directory containers.

► **To delegate Group Policy administrative tasks on a container**

1. To delegate Group Policy-related permission on a site, domain, or OU, click the appropriate container in the GPMC console.
2. In the right pane for the site, domain, or OU, click the **Delegation** tab.
3. In the drop-down list box, select the desired permission you want to manage: **Link GPOs**, **Perform Group Policy Modeling analyses**, or **Read Group Policy Results data**. Note that GP Modeling and GP Results are not available for sites.
4. To add new groups, use the **Add** button.
5. To modify the **Applies To** setting for an existing permission, right-click the user or group in the list and then select either **This container only** or **This container and all child containers**.
6. To remove an existing group or user from having the specified permission, select the user or group from the list and click the **Remove** button. Only domain administrators have permission to do this.
7. To add or remove custom permissions, click **Advanced** at the bottom-right of the details pane and select the object whose permissions you want to change. Note that setting custom permissions is *not* recommended.

Delegating Creation of GPOs

The ability to create GPOs in a domain is a permission that is managed on a per-domain basis. By default, only Domain Administrators, Enterprise Administrators, Group Policy Creator Owners, and SYSTEM can create new Group Policy objects. If the domain administrator wants a non-administrator or non-administrative group to be able to create GPOs, that user or group can be added to the Group Policy Creator Owners security group. Alternatively, you can use the **Delegation** tab on the Group Policy Objects container in GPMC to delegate creation of GPOs. When a non-administrator who is a member of the Group Policy Creator Owners group creates a GPO, that user becomes the creator owner of the GPO and can edit the GPO and modify permissions on the GPO. However, members of the Group Policy Creator Owners group cannot link GPOs to containers unless they have been separately delegated the right to do so on a particular site, domain, or OU. Being a member of the Group Policy Creator Owners group gives the non-administrator full control of only those GPOs that the user creates. Group Policy Creator Owner members do not have permissions for GPOs that they do not create.



Note

When an administrator creates a GPO, the Domain Administrators group becomes the Creator Owner of the Group Policy object. By default, Domain Administrators can edit all GPOs in the domain.

The right to link GPOs is delegated separately from the right to create GPOs and the right to edit GPOs. Be sure to delegate both rights to those groups you want to be able to create and link GPOs. By default, non-Domain Admins cannot manage links, and this prevents them from being able to use GPMC to create and link a GPO. However, non-Domain Admins can create an unlinked GPO if they are members of the **Group Policy Creator Owners** group. After a non-Domain Admin creates an unlinked GPO, the Domain Admin or someone else who has been delegated permissions to link GPOs in a container can link the GPO as appropriate.

Creation of GPOs can be delegated to any group or user. There are two methods of granting a group or user this permission:

- Add the group or user to the Group Policy Creator Owners group. This was the only method available prior to GPMC.
- Explicitly grant the group or user permission to create GPOs. This method is newly available with GPMC.

You can manage this permission by using the **Delegation** tab on the Group Policy objects container for a given domain in GPMC. This tab shows the groups that have permission to create GPOs in the domain, including the Group Policy Creator Owners group. From this tab, you can modify the membership of existing groups that have this permission, or add new groups.

Because the Group Policy Creator Owners group is a domain global group, it cannot contain members from outside the domain. Being able to grant users permissions to create GPOs without using Group Policy Creator Owners facilitates delegating GPO creation to users outside the domain. Without GPMC, this task cannot be delegated to members outside the domain.

If you require that users outside the domain have the ability to create GPOs, create a new domain local group in the domain (for example, “GPCO – External”), grant that group GPO creation permissions in the domain, and then add domain global groups from external domains to that group. For users and groups in the domain, you should continue to use the Group Policy Creator Owners group to grant GPO-creation permissions.

Adding a user to the membership of Group Policy Creator Owners and granting the user GPO-creation permissions directly using the new method available in GPMC are identical in terms of permissions.

Delegating creation of WMI filters

WMI filters are a new feature in Windows Server 2003 and Windows XP. WMI filters are created in the **WMI Filters** container in GPMC. There are two levels of permission for creating WMI filters:

- **Creator Owner:** Allows the user to create new WMI filters in the domain, but does not grant permissions on WMI filters created by other users.
- **Full Control:** Allows the user to create WMI filters, and grants full control on all WMI filters in the domain, including new filters created after users are granted this permission.

To delegate these permissions, use the **Add** button on the **Delegation** tab of the **WMI Filters** pane.

An administrator can **Add**, **Remove**, and view **Properties** for WMI Filter delegations from the **Delegation** tab. Selecting **Add** prompts for a user or group before selecting the permission level (**Creator Owner** or **Full Control**) to assign to the user or group. Selecting **Remove** prompts for confirmation that the delegation should be removed. Selecting **Properties** displays the user or group properties for that object.

Delegating permissions on individual WMI filters

GPMC allows you to delegate permissions on individual WMI filters. There are two levels of permissions that can be granted to a user or group on an individual WMI filter:

- **Edit:** Allows the user or group to edit the selected WMI filter.
- **Full Control:** Allows the user or group to edit, delete, and modify security on the selected WMI filter.

These permissions are managed by using the **Delegation** tab of a WMI filter

The **Delegation** tab shows the users and groups that have permissions on the WMI filter, their permission levels, and whether the permission is inherited from a parent container. Buttons on this tab let you add users and groups to the delegation list for the WMI filter, or remove them from this list.

Note that all users have **Read** access to all WMI filters. GPMC does not allow this permission to be removed. If the **Read** permission were removed, this can cause Group Policy processing on the destination computer to fail.

Defining Group Policy Operational Procedures

To facilitate future management of Group Policy, you should develop operational procedures to ensure that changes to GPOs are made in an authorized and controlled manner. In particular, make sure that all new GPOs and changes in existing GPOs are properly staged before deployment to your production environment. You should also create regular backups of your GPOs.

In some organizations, different teams might be responsible for managing different aspects of Group Policy. For example, a software deployment team is typically concerned with the **Software Installation (Users)** and **Software Installation (Computers)** sections of Group Policy. The remaining settings, relating to items such as scripts and Folder Redirection, are unlikely to be of interest to this team.

To reduce complexity and minimize the likelihood of introducing errors, consider creating separate GPOs for different groups of administrators.

Alternatively, you might restrict administrators to the parts of Group Policy they are authorized to change. You can use the **Restricted/Permitted Snap-ins\Extension snap-ins** policy setting to restrict the snap-ins that administrators can access. This setting is available in the Group Policy Object Editor snap-in under **User Configuration\Administrative Templates\Windows Components\Microsoft Management Console**. The **Restricted/Permitted Snap-ins\Extension snap-ins** policy pertains to the UI that is accessible by using the Group Policy Object Editor snap-in. Remember that some teams may need access to more than one type of extension snap-in. To start the Group Policy Object Editor, right-click a GPO in GPMC and then click **Edit**.

**Note**

The MMC policy settings only affect the UI that is accessible by using MMC; if Group Policy is edited by using a programmatic means, any GPO settings can be edited, including important Sysvol aspects.

For more information about these and other Group Policy settings, double-click the setting in the details pane of the Group Policy Object Editor, and then click the **Explain** tab in the policy **Properties** dialog box. Note that this information is always available by simply clicking the setting if you have **Extended View** enabled, which is the default behavior.

Specifying a Domain Controller for Editing Group Policy

In each domain, GPMC uses the same domain controller for all operations in that domain. This includes all operations on the GPOs that are located in that domain, as well as all other objects in that domain, such as OUs and security groups. When you open the Group Policy Object Editor from GPMC, it uses the same domain controller.

GPMC also uses the same domain controller for all operations on sites. This domain controller is used to read and write information about what links to GPOs exist on any given site, but information regarding the GPOs themselves is obtained from the domain controllers of the domains that host the GPOs.

By default, when you add a new domain to the console, GPMC uses the PDC emulator in that domain for operations in that domain. For managing sites, GPMC uses the PDC emulator in the user's domain by default.

The choice of domain controllers is important for administrators to consider to avoid replication conflicts. This is especially important because GPO data is located both in Active Directory and in Sysvol, which rely on independent replication mechanisms to replicate GPO data to the various domain controllers in the domain. If two administrators simultaneously edit the same GPO on different domain controllers, it is possible for the changes written by one administrator to be overwritten by another administrator, depending on replication latency.

To avoid this, GPMC uses the Operations Master token for the PDC emulator in each domain as the default. This helps ensure that all administrators are using the same domain controller and guards against data loss. However, it might not always be desirable for an administrator to use the PDC to edit GPOs. For example, if the administrator is located in a remote site, or if the majority of the users or computers targeted by the GPO are in a remote site, the administrator might choose to target a domain controller at the remote location. For example, if you are an administrator in Japan and the PDC emulator is in New York, it might be inconvenient to rely on a WAN link to access the New York PDC emulator.



Important

If multiple administrators manage a common GPO, all administrators should use the same domain controller when editing a particular GPO in order to avoid collisions in the File Replication service (FRS).

Use the **Change Domain Controller** function to specify the domain controller to be used for a given domain or for all sites in a forest. In each case, you have four options:

- **The domain controller with the Operations Master token for the PDC emulator** (the default option)
- **Any available domain controller**
- **Any available domain controller running Windows Server 2003 or later.**
- **This domain controller:** Select a specific domain controller to be used.

The selected option is used each time that you open a saved console, until you change the option.

This preference is saved in the .msc file and is used when you open that .msc file. It is generally not recommended that you use the **Any available domain controller** option unless you are performing read-only operations.

Group Policy and Slow Links

Some Group Policy is not applied when the connection speed falls below specified thresholds. Therefore, when your Group Policy solution calls for applying policy over slow links or by using remote access, you need to consider policy settings for slow link detection.

Although slow links and remote access are related, there are distinctions, and Group Policy processing varies for each. Having a computer connected to a LAN does not necessarily imply a fast link, nor does a remote access connection imply a slow link. The default value for what Group Policy considers a slow link is any rate slower than 500 Kilobits per second (Kbps). You can change this threshold using Group Policy. Group policy uses the following algorithm to measure link speed.

► How Group Policy measures link speed

1. Ping the server with 0 bytes of data and time the number of milliseconds. This value is time1. If it is less than 10 ms, exit (assume a fast link).
2. Ping the server with 2 kilobytes (KB) of uncompressible data, and time the number of milliseconds. This value is time2. The algorithm uses a compressed .jpg file to ping the server.
3. $\text{DELTA} = \text{time2} - \text{time1}$. This removes the overhead of session setup, with the result being equal to the time to move 2 KB of data.
4. Calculate Delta three times, adding to TOTAL each DELTA value. Use the following calculations:
5. $\text{TOTAL}/3 = \text{Average of DELTA in milliseconds}$.
6. $2 * (2 \text{ KB}) * (1000 \text{ ms/sec}) / \text{DELTA Average ms} = X$
7. $X = (4000 \text{ KB/sec}) / \text{DELTA Average}$
8. $Z \text{ Kbps} = ((4000 \text{ KB}) / \text{DELTA Average}) * (8 \text{ bits/byte})$
9. $Z \text{ Kbps} = 32000 \text{ kbps/Delta Average}$.

Two KB of data have moved in each direction (this is represented by the leading factor two on the left side in step six) through each modem, Ethernet card, or other device in the loop once. The resulting Z value is evaluated against the policy setting. A default of less than 500 Kbps is considered a slow link; faster than 500 Kbps is a fast link.

Administrators can use a policy setting to define a slow link for the purpose of applying Group Policy, as described in the following sections.

Specifying Group Policy for Slow Link Detection

Administrators can partially control which Group Policy extensions are processed over a slow link. By default, when processing over a slow link, not all components of Group Policy are processed.

Table 2.6 shows the default settings for processing Group Policy over slow links.

Table 2.6 Default Settings for Processing Group Policy over Slow Links

Setting	Default
Security Settings	ON (cannot be turned off)
IP Security	ON
EFS	ON
Software Restriction Policies	ON
Wireless	ON

(continued)

Table 2.6 Default Settings for Processing Group Policy over Slow Links (continued)

Setting	Default
Administrative Templates	ON (cannot be turned off)
Software Installation	OFF
Scripts	OFF
Folder Redirection	OFF
IE maintenance	ON

Administrators can use a Group Policy setting to define a slow link for the purposes of applying and updating Group Policy. The default value defines a rate slower than 500 Kbps as a slow link.

To specify settings for Group Policy slow link detection for computers, use the **Group Policy slow link detection policy** setting in the **Computer Configuration\Administrative Templates\System\Group Policy** item of the Group Policy Object Editor. The unit of measurement for connection speed is Kbps.

To set this for users, use the **Group Policy slow link detection policy** setting in **User Configuration\Administrative Templates\System\Group Policy**.

For User Profiles, the **Slow network connection timeout for user profiles** setting is located in the **Computer Configuration\Administrative Templates\System\User Profiles** item. This setting allows users to ping the server and to check the performance of the file system. This is because user profiles can be stored anywhere, and the server might or might not have IP support. Therefore, the user profile first tries to ping the server. If the server does not have IP support, it falls back to measuring the performance of the file system. You must specify connection speeds in both Kbps and milliseconds when you set this policy.



Note

If the **Do not detect slow network connections** policy setting is enabled, the **Slow network connection timeout for user profiles** policy setting is ignored.

If **Delete cached copies of roaming profiles** is enabled, there is no local copy of the roaming profile to load when the system detects a slow connection.

Setting Computer Policy for Client-Side Extensions for Processing Across Slow Links

Group Policy is implemented almost entirely as a series of client-side extensions, such as security, administrative templates, and folder redirection. There is a computer policy that allows configuring slow-link behavior for each client-side extension. You can use these policy settings to specify the behavior of client-side extensions when processing Group Policy. There is a maximum of three options for each policy setting. The **Allow processing across a slow network connection** policy option controls processing policy settings across slow links. The other two options can be used to specify that policy should not be processed in the background, or that policy be updated and reapplied even if policy settings have not changed. For more information about policy for client-side extensions, see “Specifying Group Policy for Slow Link Detection” earlier in this chapter.

Some extensions move large amounts of data, so processing across a slow link can affect performance. By default, only the administrative templates and security-related settings are processed over a slow link.

You can set the options for processing the following:

- IP Security policy
- EFS recovery policy
- Internet Explorer Maintenance policy
- Scripts policy
- Folder Redirection policy

Group Policy and Remote Access Connections

Processing of Group Policy over a remote access connection differs from processing over a slow link. Group Policy is applied during a remote access connection as follows:

- When users click to select the **Logon using dial-up connection** check box at the logon prompt, both user and computer Group Policy are applied if the computer is a member of the domain that the remote access server belongs to or trusts. However, computer-based software installation settings are not processed, nor are computer-based startup scripts executed, because computer policy is normally processed before the logon screen appears. However, in the case of using a dial-up connection, the application of computer policy is done as a background refresh during the logon process.
- When the processing of cached credentials is completed and a remote access connection is established, Group Policy is not applied, except during a background refresh.

Group Policy is not applied to computers that are members of a workgroup, because computer policy is never applied to computers that are in a workgroup.

Controlling Client-Side Extensions by Using Group Policy

Some of the Group Policy components include client-side extensions (typically implemented as .dll files) that are responsible for processing and applying Group Policy settings at the destination computers.

For each client-side extension, the GPO processing order is obtained from a list of GPOs, which is determined by the Group Policy engine during processing. Each client-side extension processes the resulting list of GPOs. For details about the processing of Group Policy, see the *Distributed Services Guide* of the *Windows Server 2003 Resource Kit* (or see the *Distributed Services Guide* on the Web at <http://www.microsoft.com/reskit>).

A computer policy exists to control the behavior of each of the Group Policy client-side extensions. Each policy includes up to three options, and some include more specific configuration options. You can set computer policies for client-side extensions by opening the **Computer Configuration/Administrative Templates/System/Group Policy** item of the Group Policy Object Editor.

You can set the following computer policy options:

- **Allow processing across a slow network connection.** Some extensions move large amounts of data, so processing across a slow link can decrease performance. By default, only the administrative templates and security settings are processed over a slow link. You can set this policy to mandate that other client-side extensions are also processed across a slow link. To control what is considered a slow link, use the **Group Policy slow link detection** setting. See “Specifying Group Policy for Slow Link Detection” earlier in this chapter.
- **Do not apply during periodic background processing.** Computer policy is applied at boot time and again every 90 minutes. User policy is applied when the user logs on to the computer and in the background approximately every 90 minutes after that. The **Do not apply during periodic background processing** option gives you the ability to override this behavior and prevent Group Policy from running in the background.



Note

The Software Installation and Folder Redirection extensions process Group Policy only at startup and when the user logs on to the network because of the risks in processing these policies in the background, when users might have applications and files open

- **Process even if the Group Policy objects have not changed.** If the GPOs on the server do not change, it is not usually necessary to continually reapply them to the destination computer except to override possible local changes. Because local administrators might be able to modify the parts of the registry where Group Policy settings are stored, you might want to reapply these settings as needed during the logon process or during periodic background processing to return the computer to the desired state.

For example, assume that Group Policy defines a specific set of security options for a file. Then a user who has administrative credentials logs on and changes those security options. The Group Policy administrator might want to set the policy option to process Group Policy even if the GPOs have not changed so that the security options specified in Group Policy are reapplied the next time policy is refreshed. The same considerations apply to applications: with this option set, if Group Policy installs an application, but the user removes the application or deletes its icon, the application is re-advertised the next time the user logs on to the computer.

By default, Security Policy settings delivered by Group Policy are applied every 16 hours (960 minutes) even if a GPO has not changed. It is possible to change this default period by using the registry entry **MaxNoGPOListChangesInterval** in the following subkey:

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{82...},

The data type of this entry is REG_DWORD and the value is number of minutes.



Caution

Do not edit the registry unless you have no alternative. The registry editor bypasses standard safeguards, allowing settings that can damage your system, or even require you to reinstall Windows. If you must edit the registry, back it up first and see the Registry Reference on the *Microsoft® Windows® Server 2003 Deployment Kit* companion CD or at <http://www.microsoft.com/reskit>.

Minimizing the Growth of DC System Volume Folders

The policy settings information in GPOs is stored in two locations: in Active Directory and in the Sysvol folder of domain controllers. The Active Directory container is also known as a *Group Policy container*, and the Sysvol folder contains the *Group Policy template*. The Group Policy container contains attributes that are used to deploy GPOs to the domain, to OUs, and to sites within the domain. The Group Policy container also contains a link to the Group Policy template, where most Group Policy settings are stored.

Information stored in the Sysvol folder includes security settings, script files, information for deploying applications that are available for Group Policy Software Installation, and Administrative Template–based Group Policy settings. Administrative Templates (.adm files) provide Group-Policy setting information for the items that appear under the Administrative Templates item in the Group Policy Object Editor.

Limiting the size of stored Group Policy information is important largely because the two storage locations use different replication mechanisms, which can cause replication conflicts. Replication conflicts are discussed in “Specifying a Domain Controller for Editing Group Policy,” earlier in this chapter.

By default, when you open the Group Policy Object Editor snap-in to edit a new or existing GPO (or when you click **Edit** after right-clicking a GPO in GPMC), the administrative computer’s .adm files for that GPO are sent to the domain controller and placed in a folder associated with the new GPO. The .adm files stored are the ones that are included with the operating system for the administrative computer (such as System.adm, Inetres.adm, Conf.adm, and Wmplayer.adm), as well as any .adm files that are added or removed by the administrator by using the **Add/Remove Templates** shortcut menu.

When an existing GPO is edited, a comparison is made of the timestamps of the local .adm files and the versions in the Sysvol folder. If the local timestamp is more recent, those files are sent to the domain controller where they are stored in the Sysvol GPO folder.

Benefits of Storing .Adm Files in the Sysvol Folder

Storing copies of .adm files in the Sysvol folder provides a consistent experience for administrators across computers. For example, if a specific set of .adm files is selected when you edit a GPO using the Group Policy Object Editor on one computer (by using **Add/Remove Templates**), these same .adm files are also included when the GPO is edited on another computer. The selected .adm files need not be installed on the second computer, because the files are retrieved from the domain controller. The list of selected .adm files is stored in the Sysvol GPO folder in the **Admfiles.ini** file.

Drawbacks of Storing .Adm Files in the Sysvol Folder

Each GPO stores its own copy of the .adm files selected for it. Because some .adm files can be large — more than 1Mb — it is possible that the Sysvol GPO folder can grow large, especially when you have a large number of GPOs.

An additional problem occurs if administrators use different language versions of the operating system. In this case, the .adm with the newest timestamp is uploaded to the Sysvol folder on the domain controller, regardless of language. This is important because non-U.S. English .adm files typically have a later timestamp than the U.S. English versions. This occurs because simply opening **Administrative Templates** in the Group Policy Object Editor on a non-U.S. English administrative computer results in the Group Policy templates being updated with the local language version of the .adm files, even if you do not actually edit any settings.

Group Policy Settings to Control Treatment of .Adm Files

To provide administrators with control how .adm files are treated, you can use the following policy settings: **Always use local ADM files for Group Policy Editor** and **Turn off automatic updates of ADM files**.

Always use local ADM files for Group Policy Object Editor

This policy setting forces the Group Policy Object Editor to use the local computer .adm files in the *systemroot\inf* directory. To access this Group Policy setting, in the Group Policy Object Editor snap-in, navigate to **Computer Configuration\Administrative Templates\System\Group Policy**. This setting is not available in the Windows 2000 family.

This setting does not alter the default treatment of .adm files when you edit a newly-created GPO: The local .adm files are always used and are copied to the Sysvol GPO folder. When you edit an existing GPO, any .adm files stored in the GPO folder on the Sysvol are ignored. When this setting is used, the Group Policy Object Editor always uses only the .adm files from the local computer (including any custom .adm files). If an .adm file is not found, the corresponding Group Policy settings are not available. This Group Policy setting can be used to ensure that language-specific versions of the .adm files on the administrative computer are used, rather than any other language version stored in the GPO folder.

Turn off automatic update of .Adm files

Enabling this policy setting prevents the system from automatically updating the .adm files in the Sysvol folder when you open the Group Policy Object Editor. This policy setting is available in the Group Policy Object Editor snap-in under **User Configuration\Administrative Templates\System\Group Policy**.

When this Group Policy setting is enabled and you edit a new GPO, no .adm files are copied from the local computer to the Sysvol GPO folder on the domain controller. Similarly, when you edit an existing GPO, no local .adm files are sent to the domain controller. This means that the Group Policy Object Editor presents only the .adm files found on the local computer, and no .adm files are copied to the domain controller.

Changing the Group Policy Refresh Interval

Administrators can change the default refresh policy interval setting by using one of these policy settings: **Group Policy Refresh Interval for Computers**, **Group Policy Refresh Interval for Domain Controllers**, or **Group Policy refresh Interval for Users**. By using these settings, you can stipulate an update rate from zero to 64,800 minutes (45 days). You can also set the policy to **Turn off background refresh of Group Policy**.



Important

When you set the refresh interval to 0 minutes, the computer tries to update Group Policy every seven seconds. Because such updates might interfere with users' work and increase network traffic, very short update intervals are appropriate only in test environments.

Group Policy Refresh Interval for Computers

This setting specifies how often Group Policy for computers is updated in the background. It specifies a background update rate only for Group Policy settings under Computer Configuration. Computer Group Policy is updated in the background every 90 minutes by default, with a random offset of 0 to 30 minutes. In addition to background updates, computer Group Policy is always updated when the system starts. This policy setting is available in the Group Policy Object Editor under **Computer Configuration\Administrative Templates\System\Group Policy**.

Group Policy Refresh Interval for Domain Controllers

This setting specifies how often Group Policy is updated in the background on domain controllers. By default, Group Policy on domain controllers is updated every five minutes. This policy setting is available in the Group Policy Object Editor under **Computer Configuration\Administrative Templates\System\Group Policy**.

Group Policy Refresh Interval for Users

This setting specifies how frequently Group Policy is updated in the background only for the Group Policy settings in the User Configuration folder. In addition to background updates, Group Policy for users is always updated when users log on. This policy is in the **User Configuration\Administrative Templates\System\Group Policy** item.

Turn off background refresh of Group Policy

This policy prevents Group Policy settings from being updated while the computer is in use. It applies to Group Policy for computers, users, and domain controllers. This policy setting is available in **Computer Configuration\Administrative Templates\System\Group Policy** item.

Running Command Line Options to Refresh Policy

From a given computer, you can refresh the settings that are deployed to that computer by using the Gpupdate.exe tool. One reason this is useful is to ensure that security settings are enforced. Table 2.7 describes parameters for Gpupdate.exe. The Gpupdate.exe tool is used in Windows Server 2003 and Windows XP environments and replaces the /refreshpolicy option previously used with the secedit command. For Windows 2000, continue to use the secedit /refreshpolicy command.

The Gpupdate.exe tool uses the following syntax:

```
gpupdate [/target:{computer|user}] [/force] [/wait:value] [/logoff] [/boot]
```

Table 2.7 Gpupdate.exe Parameters

Parameter	Description
/target:{computer user}	Depending on what target you specify, Gpupdate.exe processes the computer settings, the current user settings, or both. By default, both the computer and the user settings are processed.
/force	Reapplies all settings and ignores processing optimizations.
/wait: <i>value</i>	Specifies the number of seconds that policy processing waits to finish. The default is 600 seconds. A value of 0 means no wait; -1 means wait indefinitely.
/logoff	Logs off after the policy refresh completes. This is required for Group Policy client-side extensions that do not process on a background refresh cycle but do process when the user logs on, such as user Software Installation and Folder Redirection. This option has no effect if there are no extensions called that require the user to log off.
/boot	Restarts the computer after the policy refresh completes. This is required for those Group Policy client-side extensions that do not process on a background refresh cycle but do process when the computer starts up, such as computer Software Installation, for example. This option has no effect if there are no extensions called that require the computer to be restarted.
/?	Displays Help at the command prompt.

Using Group Policy Modeling and Group Policy Results to Evaluate Group Policy Settings

Before deploying your Group Policy solution, it is critical that you assess it to determine the effects of applying the various policy settings that you select, individually and in combination. The primary mechanism for assessing your Group Policy deployment is to create a staging environment and log on using a test account. This is the best way to understand the impact and interaction of all the applied GPO settings. Staging your Group Policy deployment is critical for creating a successful managed environment. For more information, see “Staging Group Policy Deployments” in this book.

For Active Directory networks with at least one Windows Server 2003 domain controller, you can use Group Policy Modeling in GPMC to simulate the deployment of GPOs to any destination computer running Windows 2000 Server or Professional, Windows XP Professional, or Windows Server 2003. The primary tool for viewing the actual application of GPOs is by using Group Policy Results in GPMC.

Group Policy Modeling was previously called Resultant Set of Policy (RSoP) planning mode, and Group Policy Results was previously called RSoP logging mode.

Using Group Policy Modeling to Simulate Resultant Set of Policy

The built-in Group Policy Modeling Wizard calculates the simulated net effect of GPOs. Group Policy Modeling can also simulate such things as security group membership, WMI filter evaluation, and the effects of moving user or computer objects to a different Active Directory container. The simulation is performed by a service that runs on domain controllers running Windows Server 2003. These calculated settings are reported in HTML and are displayed in GPMC on the **Settings** tab in the details pane for the selected GPO. To expand and contract the settings under each item, click **hide** or **show all** so that you can see all the settings, or only a few. To perform a Group Policy Modeling analysis, you must have at least one domain controller running Windows Server 2003, and you must have the **Perform Group Policy Modeling analyses** permission on the domain or organizational unit that contains the objects on which you want to run the query.

To run the wizard, right-click **Group Policy Modeling** (or an Active Directory container), and then click **Group Policy Modeling Wizard**. If you run it from an Active Directory container, the wizard fills in the **Container** fields for user and computer with the LDAP distinguished name of that container.

When you have answered all the questions in the wizard, your answers are displayed as if they were from a single GPO. They are also saved as a query represented by a new item under the **Group Policy Modeling** item. The display also shows which GPO is responsible for each setting, under the heading **Winning GPO**. You can also see more detailed precedence information (for example, which GPOs attempted to set the settings, but did not succeed). To do so, right-click the item, and then click **Advanced View**. This starts the traditional RSoP snap-in. Each setting has a **Precedence** tab.

Keep in mind that modeling does not include evaluating any LGPOs. Because of this, in some cases you might see a difference between the simulation and the actual results.

To save the results of the modeling, right-click the query, and then click **Save Report**.

Using Group Policy Results to determine Resultant Set of Policy

Use the Group Policy Results Wizard to see what Group Policy settings are actually in effect for a user or computer by gathering RSoP data from the destination computer. In contrast to Group Policy Modeling, Group Policy Results reveals the actual Group Policy settings that were applied to the destination computer. The target must be running Windows XP Professional or later.

The settings are reported in HTML and are displayed in a GPMC browser window on the **Summary** and **Settings** tabs in the details pane for the selected GPO. You can expand and contract the settings under each item by clicking **hide** or **show all** so that you can see all the settings, or only a few. To remotely access Group Policy Results data for a user or computer, you must have the **Remotely access Group Policy Results data** permission on the domain or organizational unit that contains the user or computer, or you must be a member of a local Administrator's group on the appropriate computer and must have network connectivity to the destination computer. To delegate Group Policy Results, you need the Windows 2003 Server schema in your Active Directory. To update your schema, run **ADPrep /forestprep** on the domain controller with the schema operations master role.

To run the wizard, right-click the **Group Policy Results** container, and then click **Group Policy Results Wizard**.

When you have answered all the questions in the wizard, GPMC creates a report that shows the resultant set of policy for the user and computer you entered in the wizard. The display shows which GPO is responsible for each setting on the **Settings** tab, under the heading **Winning GPO**.

You can save the results by right-clicking the query and choosing **Save Report**.

Using Gpresult.exe to Evaluate Policy Settings

You can run Gpresult.exe on the command line of any remote computer within the scope of your management to get the same data you can get by using GPMC Group Policy Results. By default, Gpresult.exe returns settings in effect on the computer on which it runs.

For Windows Server 2003 and Windows XP Professional, Gpresult.exe uses the following syntax:

```
gpresult [/s computer [/u domain\user /p password]] [/user TargetUserName] [/scope {user|computer}] [/v] [/z]
```

Table 2.8 describes the parameters for Gpresult.exe.

Table 2.8 Gpresult.exe Parameters

Parameter	Description
/s <i>computer</i>	Specifies the name or IP address of a remote computer. (Do not use backslashes.) The default is the local computer.
/u <i>domain\user</i>	Runs the command using the account permissions of the user that is specified by User or Domain\User. The default is the permissions of the current logged-on user on the computer that issues the command.
/p <i>password</i>	Specifies the password of the user account that is specified in the /u parameter.
/user <i>TargetUserName</i>	Specifies the user name of the user whose RSoP data is to be displayed.
/scope { <i>user computer</i> }	Displays either user or computer results. Valid values for the /scope parameter are user or computer. If you omit the /scope parameter, gpresult displays both user and computer settings.
/v	Specifies that the output display verbose policy information.
/z	Specifies that the output display all available information about Group Policy. Because this parameter produces more information than the /v parameter, redirect output to a text file when you use this parameter (for example, gpresult /z >policy.txt).
/?	Displays help at the command prompt.

► **To run Gpresult.exe on your computer**

1. Click **Start**, click **Run**, type **cmd**, and then press ENTER.
2. Type **gpresult /z>gp.txt** to write the output to a text file that is named Gp.txt.
3. Type **notepad gp.txt** to open the text file.

Note that using Group Policy Results is recommended over using Gpresult.exe. GPResult.exe is primarily useful if you desire command-line *presentation* of resultant set of policy data. If you require command-line access to RSOP data but not command-line presentation of the data, you can simply run a script based on the GPMC interfaces to generate an RSOP report in the form of an .htm file.

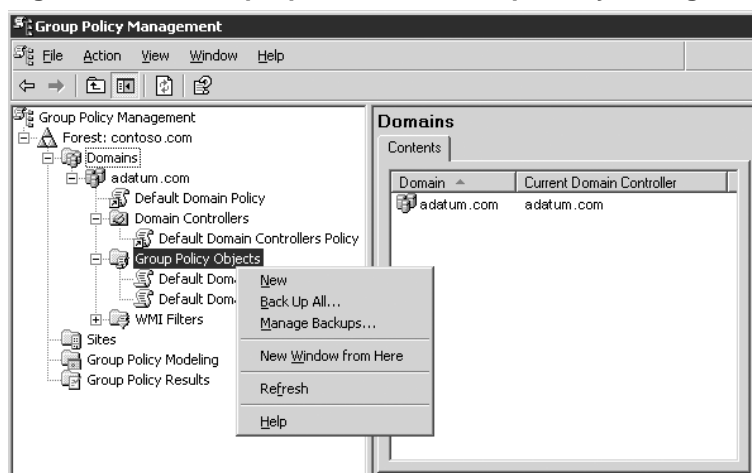
Backing up, Restoring, Migrating, and Copying GPOs

GPMC provides mechanisms for backing up, restoring, migrating, and copying existing GPOs. This is very important for maintaining your Group Policy deployments in event of error or disaster. It helps you avoid having to manually recreate lost or damaged GPOs and then go through the planning, testing, and deployment phases again. Part of your ongoing Group Policy operations plan should include regular backups of all GPOs. Inform all Group Policy administrators about how to use GPMC to restore GPOs.

GPMC also provides for copying and importing GPOs, both from the same domain and across domains. You can use GPMC to migrate an existing GPO, for example, from an existing domain into a newly deployed domain. You can either copy GPOs or import settings from one GPO into another GPO. This can save you a lot of time and trouble by enabling you to re-use the contents of existing GPOs. Copying GPOs enables you to move straight from the staging phase to production, provided you have the proper trust between the environments. Import allows you to transfer settings from a backed-up GPO into an existing GPO, and is especially useful in situations where there is no trust between the source and destination domains. If you want to reuse existing GPOs, copying also allows you to conveniently move GPOs from one production environment to another.

Using GPMC to Work with GPOs

To create GPO backups, you must have at least **Read** access to the GPOs and **Write** access to the folder in which the backups are stored. See Figure 2.10 to help you identify the items referred to in the procedures that follow.

Figure 2.10 Backup Options in the Group Policy Management Console User Interface

Using GPMC to Back up GPOs

The backup operation backs up a live GPO to the file system. The location of the backup can be any folder to which you have write access. After backing-up GPOs, you must use GPMC to display and manipulate the contents of your backup folder, either by using the GPMC UI or programmatically by using a script. Do not interact with backed-up GPOs directly through the file system. Once backed up, archived GPOs can be processed by the **Import** and **Restore** operations.

Note that you can back up multiple instances of the same GPO to the same location — GPMC uniquely identifies each backup instance and provides mechanisms to allow you to pick which instance of the archived GPO you want to work with. For example, you can choose to display only the most recent backups when viewing the contents of a backup folder through GPMC. This can be useful when you make backups of a GPO after changing it, and later need to restore a previous version of that GPO.

► To back up all GPOs in a domain

1. In the GPMC console tree, expand the forest or domain that contains the GPOs you want to back up.
2. Right-click the **Group Policy Objects** container.
3. In the context menu, click **Back Up All**.
4. In the **Backup Group Policy Object** dialog box, enter the path to the location at which you want to store the GPO backups. Alternatively, you can click **Browse**, locate the folder in which you want to store the GPO backups, and then click **OK**.
5. Type a description for the GPOs that you want to back up, and then click **Backup**.
6. After the operation completes, click **OK**.

► **To back up a specific GPO**

1. In the **Group Policy Objects** container, right-click the GPO you want to back up.
2. In the context menu, click **Back Up**.
3. In the **Backup Group Policy Object** dialog box, enter the path to the location at which you want to store the GPO backup. Alternatively, you can click **Browse**, locate the folder in which you want to store the GPO backup, and then click **OK**.
4. Type a description for the GPO that you want to back up, and then click **Backup**.
5. After the operation completes, click **OK**.

► **To manage GPO backups**

1. In the GPMC console tree, expand the domain that contains the GPOs that you want to back up.
2. Right-click **Group Policy Objects** container.
3. In the **Manage Backups** dialog box, click **Browse**, locate the folder that contains your GPO backups, and then click **OK**.



Important

You should secure backed-up GPOs by ensuring that only authorized administrators have permission to access the folder to which you are saving GPOs. Use good security on the file system where they are backed up.

Using GPMC to Restore GPOs

You can also restore GPOs. This operation takes a backed-up GPO and restores it to the same domain from which it was backed up. You cannot restore a GPO from backup into a domain different from the GPO's original domain.

► **To restore a previous version of an existing GPO**

1. In the GPMC console tree, expand the forest or domain that contains the GPOs you want to restore.
2. Expand the **Group Policy Objects** container, right-click the GPO you want to restore to a previous version, and then click **Restore from Backup**.
3. When the Restore Group Policy Object Wizard appears, follow the instructions and provide the appropriate information about the backed-up GPO that you want to restore, and then click **Finish**.
4. After the Restore Group Policy Object Wizard completes the restore operation, click **OK**.

► **To restore a deleted GPO**

1. Right-click the **Group Policy Objects** container and then select the **Manage Backups** option from the context menu.
2. In the **Manage Backups** dialog box, click **Browse**, and then locate the file system that contains your backed-up GPOs.
3. Select the GPO that you want to restore, and then click **Restore**.
4. When you are prompted to confirm the restore operation, click **OK**.



Note

Settings that are stored outside the GPOs, such as WMI filters and IPsec policies are not backed up or restored during these processes. However, links to WMI filters and IPsec are stored in the GPO, and these are backed up as part of the GPO. During restore, the links are preserved if the underlying object still exists in Active Directory.

Using GPMC to Copy GPOs and Import GPO Settings

GPMC allows you to copy GPOs, both in the same domain and across domains, as well as import Group Policy settings from one GPO to another. Perform these operations as part of your staging process prior to deployment in your production environment. These operations are also useful for migrating GPOs from one production environment to another.

Although the collection of settings which comprises a GPO is logically a single entity, the data for a single GPO is stored in multiple locations and in a variety of formats; some data is contained in Active Directory and other data is stored in the Sysvol folder on domain controllers. This means that you cannot simply copy GPOs by copying a folder from one computer to another. However, GPMC provides built-in support that allows you to do this safely and relatively simply.

A copy operation copies an existing, live GPO to the desired destination domain. A new GPO is always created as part of this process. The destination domain can be any trusted domain in which you have the rights to create new GPOs. Simply add the desired forests and domains in GPMC and use GPMC to copy and paste (or drag and drop) the desired GPOs from one domain to another. To copy a GPO, you must have permission to create GPOs in the destination domain.

An additional option available when copying GPOs is to copy the Discretionary Access Control List (DACL) on the GPO in addition to the settings within the GPO. This is useful for ensuring that the new GPO that is created as part of the copy operation has the same security filtering and delegation options as the original GPO.

Importing a GPO allows you to transfer settings from a backed-up GPO to an existing GPO. Importing a GPO transfers only the GPO settings; it does not modify the existing security or links on the destination GPO. Importing a GPO is useful for migrating GPOs across untrusted environments, because you only need access to the backed-up GPO, not the actual GPO. Because an import operation only modifies settings, Edit permissions on the destination GPO are sufficient to perform the operation.

When copying or importing a GPO, you have the option of specifying a migration table if the GPO contains security principals or UNC paths that might need to be updated to new values in the target domain. Use the Migration Table Editor to create and edit migration tables; migration tables are described in the next section, “Using GPMC to Migrate GPOs.”

► **To copy a GPO**

1. In the GPMC console tree, right-click the GPO that you want to copy, and then click **Copy**.
 - To place the copy of the GPO in the same domain as the source GPO, right-click the **Group Policy Objects** container, and then click **Paste**.
 - To place the copy of the GPO in a different domain (either in the same or a different forest), expand the destination domain, right-click the **Group Policy Objects** container, and then click **Paste**.
2. If you are copying within a domain, click **Use the default DACL for new GPOs** or **Preserve the existing DACL**, and then click **OK**.
3. If you are copying to or from another domain, answer all the questions in the cross-domain copying wizard that appears, and then click **Finish**.

► **To import settings from a backed up GPO into a GPO**

1. In the GPMC console tree, expand the domain that contains the GPO into which you want to import settings.
2. Expand the **Group Policy Objects** container, right-click the GPO, and then click **Import Settings**.
3. When the Import Settings Wizard appears, follow the instructions and provide the appropriate information about the backed up GPO that contains the settings you want to import, and then click **Finish**.

Using Migration Tables

Because some data in a GPO is domain-specific and might not be valid if copied directly to another domain, GPMC introduces *migration tables*. Migration tables are stored with the file name extension `.migtable`, and are actually XML files.

A migration table is a file that maps references to users, groups, computers, and UNC paths in the source GPO to new values in the destination GPO. The migration table consists of one or more mapping entries. Each mapping entry consists of a source type, source reference, and destination reference. If you specify a migration table when performing an import or copy, each reference to the source entry is replaced with the destination entry when the settings are written into the destination GPO. To use a migration table, the destination references specified in the migration table must already exist.

To examine a sample migration table, see **program files\GPMC\Scripts\SampleMigrationTable.migtable** on a computer where GPMC is installed. You do not need to know XML to create or edit migration tables; GPMC provides the Migration Table Editor for manipulating migration tables.

You can use migration tables to update security principals and UNC paths to new values as part of the import or copy operation.

The following items can contain security principals and can be modified using a migration table.

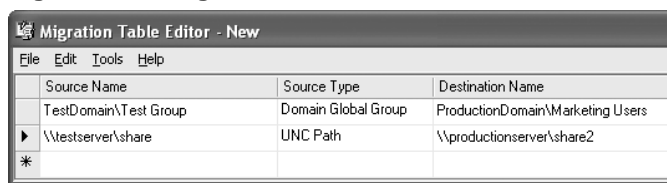
- Security policy settings of the following types:
 - User rights assignment
 - Restricted groups
 - System services
 - File system
 - Registry
- Advanced folder redirection settings
- The GPO DACL, if it is preserved during a copy operation
- The DACL on software installation objects, which is only preserved if the option to copy the GPO DACL is specified

Also, the following items can contain UNC paths, which might need to be updated to new values as part of the import or copy operation, because servers in the original domain might not be accessible from the domain to which the GPO is being migrated:

- Folder redirection Group Policy settings
- Software installation Group Policy settings
- References to scripts (such as for logon and startup scripts) that are stored outside the GPO. The script itself is not copied as part of the GPO copy or import operation, unless the script is stored inside the source GPO.

A migration table is a simple table that specifies a mapping between a source value and a destination value. Figure 2.11 shows a migration table in the Migration Table Editor in GPMC.

Figure 2.11 Migration Table Editor



Source Name	Source Type	Destination Name
TestDomain\Test Group	Domain Global Group	ProductionDomain\Marketing Users
▶ \\testserver\share	UNC Path	\\productionserver\share2
*		

The purpose of this table is to perform, during the copy or import operation, conversion of the references in a GPO to new references that will work in the target domain.

For more information about using migration tables, see “Staging Group Policy Deployments,” in this book, and see the white papers available from the Administering Group Policy with GPMC link and the Migrating GPOs Across Domains by Using GPMC link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Maintaining Group Policy

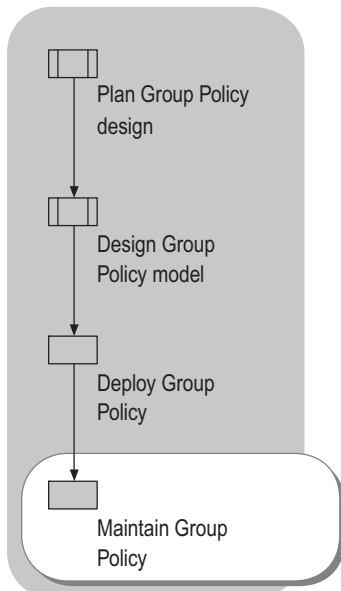
After deployment, your Group Policy implementation might need routine maintenance and modification as your organization and its needs evolve and as your experience with Group Policy grows. By establishing control procedures for creating, linking, editing, importing settings into, backing up, and restoring Group Policy objects, you can minimize help desk and support calls arising from poorly planned Group Policy deployments. You can also simplify troubleshooting GPOs and help lower the total cost of ownership for computers in your network.

By establishing GPO control mechanisms, you can create GPOs that:

- Conform to corporate standards.
- Ensure that policy settings do not conflict with those set by others.

Figure 2.12 illustrates the place of this step in the process of designing a Group Policy infrastructure.

Figure 2.12 Maintaining Group Policy



To assist with troubleshooting GPOs, you can use the GPMC Group Policy Results Wizard to identify possible Group Policy deployment errors. For more information about this tool, see “Using Group Policy Modeling and Group Policy Results to Evaluate Group Policy Settings” earlier in this chapter. You can also use the GPMC Group Policy Modeling Wizard to evaluate the consequences of new Group Policy settings prior to deploying them to your production environment.

Whenever you deploy new technology solutions, such as wireless networking, you need to revisit your Group Policy configurations to ensure compatibility with new technology. To help manage various technologies, Group Policy offers settings such as those for Wireless Network IEEE (802.11) Policies options in **Security Settings**, Terminal Services in **Administrative Templates**, and settings for many other technologies.

Modifying Group Policy settings can have significant consequences. When performing Group Policy maintenance, you need to take reasonable precautions to test proposed changes and evaluate their effects in a staging environment prior to deployment.

Group Policy Considerations for Renaming a Domain

Domain names are a critical part of the proper functioning of a Group Policy implementation. In the Windows Server 2003 family, administrators can rename a domain. This is accomplished by using the Rename Domain Tools available for download from the Windows Server 2003 Domain Rename Tools link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>. The Domain Rename tools provide a secure and supported methodology to rename one or more domains (as well as application directory partitions) in a deployed Active Directory forest.



Important

Be sure to back up all your GPOs using GPMC after domain rename is complete. Backups made prior to domain rename cannot be used for **Restore** after a domain rename.

Renaming one or more domains is a complex process that requires thorough planning and understanding of the domain rename procedures. You must also modify any affected GPOs so that they work correctly. To modify the GPOs, use the Gpfixup.exe tool, which is included with the Domain Rename tools. Gpfixup.exe repairs GPOs as well as GPO references in each renamed domain. It is necessary to repair the GPOs and the Group Policy links after a domain rename operation in order to update the old domain name embedded in these GPOs and their links.



Important

Renaming a domain is a complex process that requires thorough planning and understanding of the domain rename procedures. For more information about the domain renaming process, see the Windows Server 2003 Domain Rename Tools link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Using Scripts to Manage Group Policy

GPMC provides a comprehensive set of COM interfaces that you can use to script many of the operations supported by the snap-in. To help you get started, the GPMC installation includes sample scripts that use these interfaces. The sample scripts are installed in the \Program Files\GPMC\Scripts\ folder. Full details about the scripting interfaces are documented in the Group Policy Management Console SDK, is installed as Gpmc.chm in Program Files\GPMC\Scripts\ on any computer where you have installed GPMC. The GPMC SDK is also located in the Platform SDK. For more information about scripting GPMC operations, see the *Distributed Services Guide* of the *Windows Server 2003 Resource Kit* (or see the Distributed Services Guide on the Web at <http://www.microsoft.com/reskit>).

The sample scripts form the basis for a scripting toolkit that you can use to solve specific administrative problems. For example, you can run queries to find all GPOs in a domain that have duplicate names, or to generate a list of all GPOs in a domain whose settings are disabled or partially disabled. The scripts also illustrate some key scripting objects and methods to provide an overview of the many administrative tasks that you can accomplish with the Group Policy Management snap-in. You can modify and distribute the sample scripts in accordance with the terms of the End User License Agreement.

All of the scripts run from the command line. Running a script with the `/?` switch displays the usage for that script.

The sample scripts echo output to the command window and must be executed by using Cscript.exe. If Cscript.exe is not your default scripting host, you will need to explicitly specify Cscript.exe on the command line. For example, type `d: \Program Files\GPMC\Scripts>cscript ListAllGPOs.wsf`.

To make Cscript the default scripting host, type `cscript //h:cscript` at the command line.

Many of the sample scripts rely on a library of common helper functions contained in the file `Lib_CommonGPMCFUNCTIONS.js`. If you copy these scripts to another location, you must also copy this library file to that location in order for the script samples to work.

Additional Resources

These resources contain additional information related to this chapter.

Related Information

- The *Distributed Services Guide* of the *Windows Server 2003 Resource Kit* (or see the Distributed Services Guide on the Web at <http://www.microsoft.com/reskit>) for more information about Group Policy.
- “Deploying Security Policy” in this book.
- “Deploying a Managed Software Environment” in this book.
- “Staging Group Policy Deployments,” in this book.

- “Designing the Active Directory Logical Structure” in *Designing and Deploying Directory and Security Services* of this kit.
- “Designing and Deploying File Servers” in *Planning Server Deployments* of this kit.
- “Planning an Active Directory Deployment Project” in *Designing and Deploying Directory and Security Services* of this kit.
- “Deploying Distributed Security Services” in *Designing and Deploying Directory and Security Services* of this kit.
- The *Distributed Services Guide* of the *Windows Server 2003 Resource Kit* (or see the Distributed Services Guide on the Web at <http://www.microsoft.com/reskit>) for information about Active Directory.
- The Implementing Common Desktop Management Scenarios link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources> for information about using the sample Group Policy objects included on the Windows Server 2003 Deployment Kit companion CD.
- The Best Practice Active Directory Design for Managing Windows Networks link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.
- The Group Policy Management Console White Paper link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.
- The Migrating GPOs Across Domains by Using GPMC link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Related Help Topics

For best results in identifying Help topics by title, in Help and Support Center, under the **Search** box, click **Set search options**. Under **Help Topics**, click to select the **Search in title only** check box.

- “Group Policy” in Help and Support Center for Windows Server 2003.
- Help in GPMC for detailed information about using GPMC to help deploy Group Policy and troubleshoot your deployment.
- Help for specific Group Policy settings in the default **Extended** view in Group Policy Object Editor (select a Group Policy setting to see detailed information for that setting).
- Command-line reference A-Z in Help and Support Center for Windows Server 2003, for more information about command-line tools such as Dcgpofix.exe.
- Type **hh system.chm** at the command line to see the full description of Group Policy settings. If you open this Help file on a Windows XP Professional–based computer, you will only see settings for Windows 2000 and Windows XP Professional; if you open this Help file on a computer running Windows 2003 Server, you will see settings for Windows 2000, Windows XP Professional, and Windows 2003 Server.

Staging Group Policy Deployments



Microsoft® Windows® Server 2003 Group Policy provides powerful capabilities for deploying configuration changes across the enterprise. As with any other change within the enterprise, Group Policy deployments and ongoing updates require careful planning and testing to ensure a highly available and secure infrastructure. By using features included in the Group Policy Management Console (GPMC), you can create a test/staging/production deployment process that ensures predictability and consistency during Group Policy deployments.

In This Chapter

Overview of Group Policy Staging.....	120
Creating the Staging Environment.....	126
Synchronizing the Staging and Production Environments	130
Testing Group Policy in the Staging Environment.....	136
Preparing for Deployment to Production	140
Deploying Staged GPOs to the Production Environment.....	148
Additional Resources.....	156

Related Information

- For more information about Group Policy and GPMC features and capabilities, see “Deploying a Group Policy Infrastructure” in this book.
- For more information about using IntelliMirror to create a managed environment “Planning a Managed Environment” in this book.

Overview of Group Policy Staging

Group Policy is a powerful tool for configuring Microsoft® Windows® 2000, Windows® XP Professional, and Windows Server 2003 operating systems across the enterprise. This ability to affect configurations across hundreds or even thousands of computers necessitates good change management practices to ensure that the changes made to a Group Policy object (GPO) produce the expected results for the intended targets — users and computers — in infrastructures that use the Active Directory® directory service.

Most enterprises have change management processes in place to ensure that any new configurations or deployments of production systems go through rigorous testing in a non-production environment prior to moving them into the production environment.

In many change management processes, enterprises differentiate between a test environment, which is used to test changes, and a staging environment, which is a pristine environment that resembles production and is the last stop for a change before it is deployed to production. In this chapter, the terms test and staging are used interchangeably, without differentiating between them as physical environments. You can, however, use the techniques described in this chapter to create separate test and staging environments if your change management processes require them.

This kind of change management process is equally important for Group Policy changes because Group Policy is capable of affecting everything from registry settings to security settings to deployed software on a workstation or server. In addition to the many configuration settings that Group Policy accommodates, GPOs can be linked to a number of different scopes, and their effect can be filtered by users, computers or security groups. The ability to stage GPOs in a pre-production test environment and then test the various ways that they can be deployed prior to committing them to live users and computers is critical to ensure reliable, robust operation of your Windows-based infrastructure.

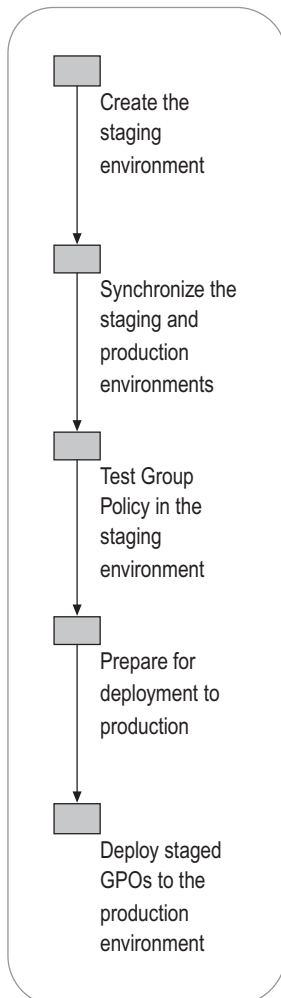
The creation of a staging environment is critical to any successful deployment of Group Policy within your Active Directory-based infrastructure. There are several options that you can choose from to create such an environment. These options are enabled by using features within the Group Policy Management Console (GPMC). GPMC runs on 32-bit computers running a member of the Windows Server 2003 family operating system or Windows XP Professional with Service Pack 1 (SP1). GPMC consists of a set of scriptable interfaces for managing Group Policy and an MMC-based user interface (UI). The UI integrates all previous Group Policy tools into a unified Group Policy-management console. GPMC can manage both Windows Server 2003 and Windows 2000 Active Directory-based domains, although some features are available only in Active Directory environments running Windows Server 2003.

GPMC console-based features and accompanying Windows Script Host (WSH) scripts give you the ability to create a staging environment that mimics your production environment. You can then use the staging environment to test new or changed GPOs. Once those GPOs are validated, you can use GPMC to migrate them to your production domains.

Group Policy Staging Process

The process for staging Group Policy involves creating a staging environment that mimics the production environment, testing new Group Policy settings in the staging environment, and then deploying those settings in the production environment. The specific deployment approach you use depends on the configuration of your staging environment. Figure 3.1 shows the steps in the Group Policy staging process.

Figure 3.1 Staging Group Policy



Initially, assembling a staging environment for Group Policy is simply a matter of identifying available hardware that can be used in creating an infrastructure that is similar to your production environment, and then setting up the appropriate logical structure. You can then use tools in GPMC to import production Group Policy into the staging environment. Once you have created the environment, testing Group Policy involves implementing changes and measuring their effect on test users and computers that mimic production users and computers. Once you have validated your changes, you can again use tools in GPMC to migrate changed or new Group Policy settings to your production environment.

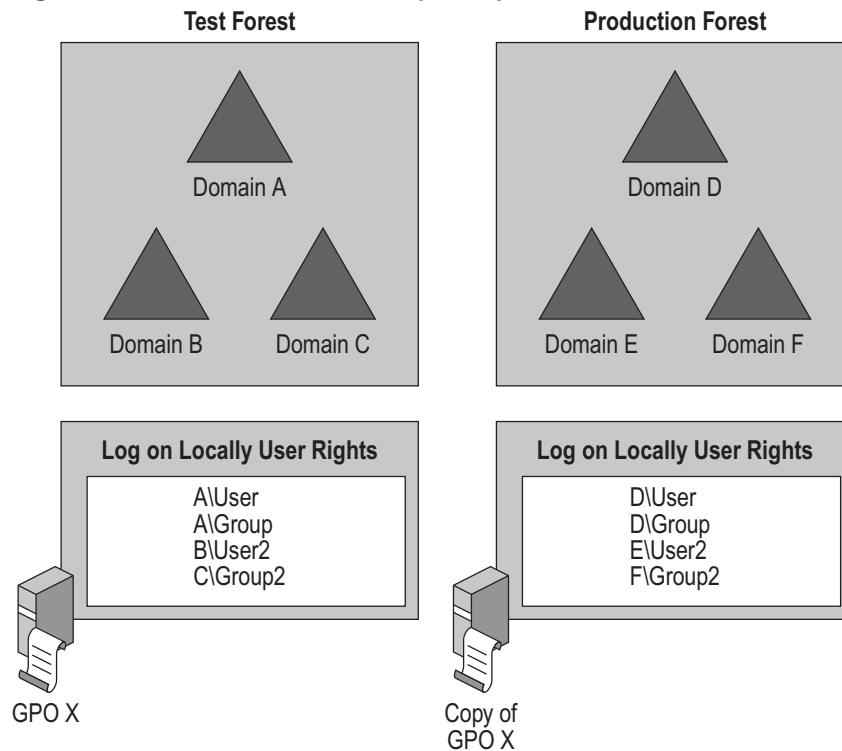
On an ongoing basis you need to maintain Group Policy and continue to evaluate changes. Consequently, you need to keep the staging environment synchronized with the production environment over time. You can use GPMC tools such as the supplied scripts and the console-based Group Policy backup, copy and import features to maintain the staging environment over time.

GPMC Staging Technology Background

GPMC is a new tool for managing Group Policy. It includes several features for creating and maintaining Group Policy, including the Group Policy Modeling Wizard for planning Group Policy deployments, the Group Policy Results Wizard for viewing GPO interaction and for troubleshooting, and the ability to use a single MMC interface to manage Group Policy across your organization, including importing and exporting, copying and backing up and restoring GPOs. For detailed information about GPMC features and capabilities, see Help in GPMC, and see “Deploying a Group Policy Infrastructure” in this book. For staging Group Policy, the most important GPMC tools are those that allow you to stage and migrate GPOs between forests and domains.

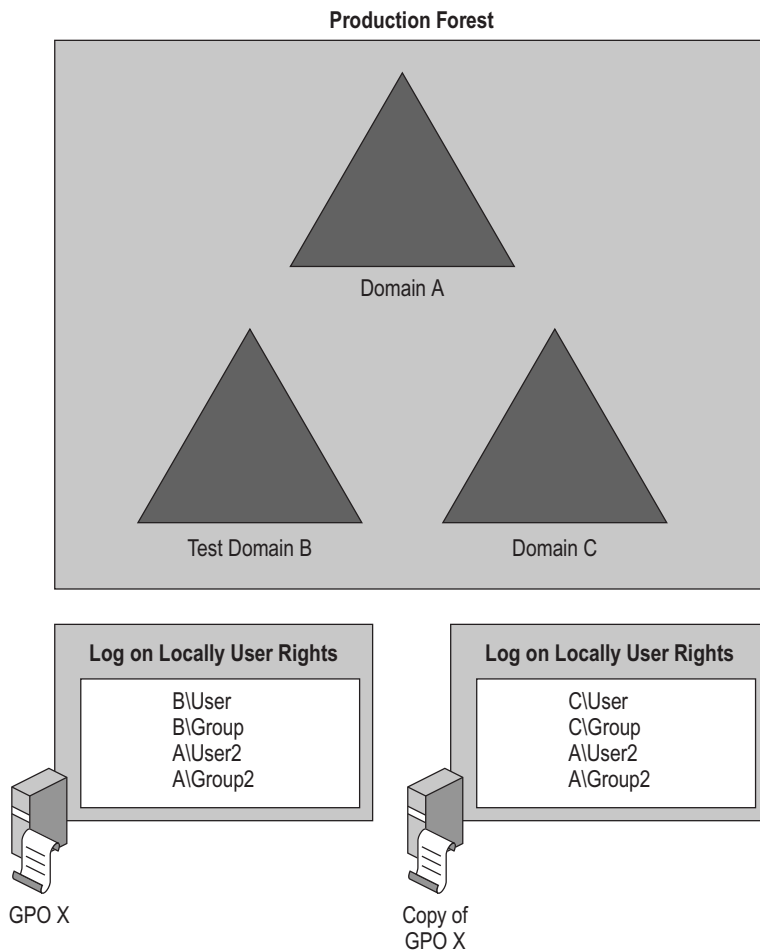
Backup and Import

GPMC provides the ability to back up one or more GPOs. These backups can then be used to restore an individual GPO to its previous state (using the restore option), or backups can be imported into an existing GPO, overwriting any previous policy settings. The restore operation is used only to restore a GPO into the same domain from which it was backed up. By contrast, the import operation is used in cases where the backup was made from any GPO in the same domain, a different domain or even in a different untrusted forest, such as a test forest isolated from the production forest. Note that while both restore and import operate on previously backed-up GPOs, restore has some additional capabilities that are specific to a restore operation. You will use the backup and import operations and the copy operation to stage and migrate GPOs into your production environment. Figure 3.2 illustrates the import operation. In this case, GPO X in a test forest contains a number of security principals who are assigned the Log on locally user right. This GPO is backed up and then imported into the production forest. During the import operation, the original security principals are mapped to new ones that exist in the production domain.

Figure 3.2 Cross-Forest GPO Import Operation

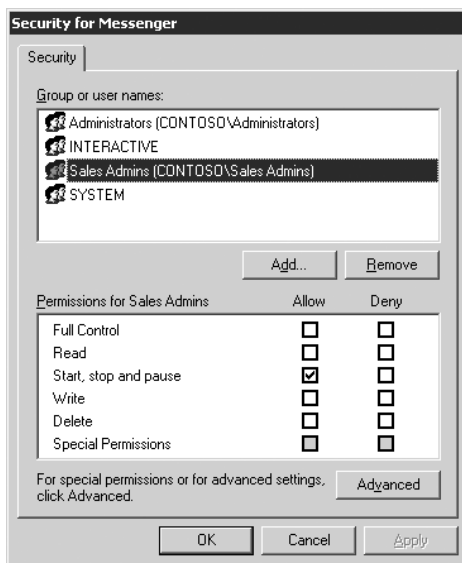
Copy

Using the copy capability in GPMC, you can right-click a GPO, copy it from one domain, and paste it into a new domain. In a copy operation, when you copy a GPO into a new domain, a new GPO is created. This differs from the import operation, which erases and then overwrites an existing GPO. Copy operations require that the destination domain is trusted by the source domain. In addition, the administrator performing the copy operation must have rights to read the source GPO in order for the copy operation to succeed. With both import and copy operations, GPMC supports the ability to perform security principal and UNC mapping between references to those objects in the source and destination GPOs. Figure 3.3 illustrates a copy operation. In this case a GPO is migrated from Domain B to Domain C and some of its associated security principals are mapped to new principals on Domain C.

Figure 3.3 Copy Operation Between Domains in a Production Forest

Migration Tables

GPOs can contain references to security principals and UNC paths as part of a policy setting. For example, within security settings policies, you can control who can start and stop a particular Windows service by using the Group Policy Object Editor to specify a user or user group for that policy. Figure 3.4 illustrates the security settings that can be applied to the Messenger service. In this case, these security settings can be mapped from security principals in the staging environment to security principals in a production environment by using migration tables.

Figure 3.4 Security Principals on the Messenger Service

In addition, a GPO itself has an associated Discretionary Access Control List (DACL) that is used to control which computers, users, or groups process a GPO and which users can create, modify, and edit the GPO. The security principals associated with the DACL on a GPO can also be taken into consideration when the GPO is deployed from one domain to another.

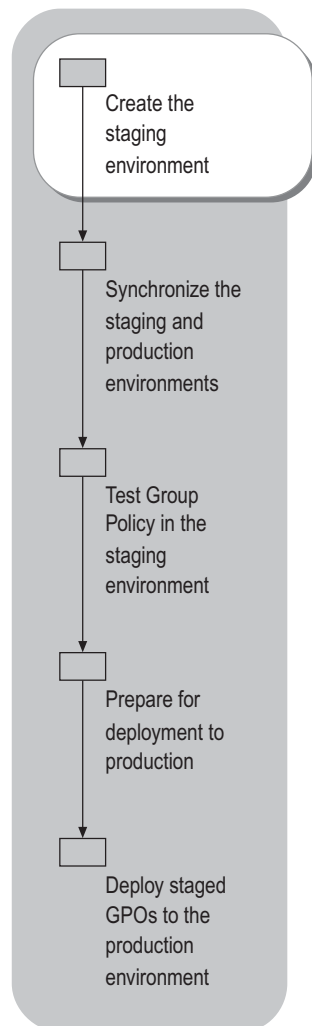
Migration tables also support mapping of UNC paths, which might exist in Software Installation, Folder Redirection, or Scripts policy. To deal with any differences in these paths between the test and production environments, you can use migration tables to replace server and share names as you migrate Group Policy.

If a GPO created in another domain or forest is migrated to your production environment, you need a way of modifying the associated security principal references to reflect the references found in the production domain. GPMC provides a Migration Table Editor (MTE) that you can use to create a mapping file for security principals and UNC paths. MTE creates an XML format file with a .migtable extension; this file specifies the source and destination security principals or UNC paths for a GPO migration. For more information about MTE, see “Creating Migration Tables” later in this chapter.

Creating the Staging Environment

The first step in staging and deploying Group Policy is the creation of the staging environment. This involves building a test infrastructure that mirrors that of production and allows you to test new or changed Group Policy settings without affecting production users and computers. Figure 3.5 illustrates this step in the staging process.

Figure 3.5 Creating the Staging Environment



At this point, you need to make decisions about the placement of your staging environment and its trust relationships to your production environment. You can choose to create:

- A staging domain within the production forest.
- A staging forest with no trusts to the production forest.
- A staging forest with trusts to the production forest.

Each option has its benefits and drawbacks, as described in Table 3.1.

Table 3.1 Choosing a Staging Approach

Approach	Advantages	Disadvantages
Staging Domain within Production Forest	<ul style="list-style-type: none"> • Can use GPMC copy operation to move GPOs between staging and production environments. • Can leverage existing production infrastructure services (for example, DNS, DHCP). • Might require less hardware to implement than a completely isolated environment that requires supporting infrastructure. • Easier to keep synchronized with production environment because all settings and services are in the same forest. • Might require less use of migration tables if migrating from domain to domain in the production forest (for example, some security principals can be re-used regardless of domain). 	<ul style="list-style-type: none"> • Might not be sufficiently isolated from production environment to ensure testing does not affect it (for example, site-linked GPOs cannot easily be tested because sites span domains within a forest). • Might prove restrictive if changes to the environment are required for testing.
Staging Forest with no trusts to Production Forest	<ul style="list-style-type: none"> • Completely isolated from production environment; provides maximum protection from test GPOs affecting production computers and users. • No security overlap between staging and production; administrators in staging and production forests need not have access to both forests. • Provides flexibility; administrators can experiment freely with settings and configurations without affecting the production environment. 	<ul style="list-style-type: none"> • Difficult to keep synchronized with production forest. • Without trusts, movement of data and settings between forests is more cumbersome. • Migration Tables are required to move GPOs that contain security principals or UNC paths from staging to production. • Cannot use GPMC copy operation to migrate GPOs; must use GPMC import.

(continued)

Table 3.1 Choosing a Staging Approach (*continued*)

Approach	Advantages	Disadvantages
Staging Forest with trusts to Production Forest	<ul style="list-style-type: none"> • Can use GPMC copy operation to move GPOs between staging and production environments. • Somewhat isolated from production environment. • Provides flexibility; administrators can experiment freely with settings and configurations without affecting the production environment. • Might not need migration tables to map UNC paths, since all paths could be available via current trusts. 	<ul style="list-style-type: none"> • Difficult to keep synchronized with production forest. • Trusts between staging and production environments allow users in one environment to access resources in the other. • Migration Tables required to move GPOs that contain security principals from the staging environment to the production environment.

Weigh the advantages and disadvantages described in Table 3.1 when making your choice of a staging approach. Ultimately, your choice depends on your own unique requirements. Once you have made your choice, you are ready to determine the hardware requirements for the staging environment.

Hardware Requirements

Regardless of the approach you choose, it will be necessary to dedicate some additional hardware to the construction of your staging environment. How much hardware you need depends upon the kinds of testing you need to do and how specific your Group Policy testing requirements are. For example, if your production forest has workstations located across slow network links from your domain controllers, this fact can affect the application of Group Policy because some Group Policy settings are not applied across slow links. It is important that your test environment reflect this situation for you to get an accurate picture of how your production environment will be impacted by changes in Group Policy. GPMC can help in such a situation, for example, by providing the capability to model the impact of slow links on GPO application. However, you might not be able to fully mirror your production environment unless you dedicate sufficient systems and network hardware to the staging environment. Your goal is to produce a testing and staging environment that reflects what computers and users in your production environment will see when new or changed GPOs are applied.

Preparing the Staging Environment

Once you have chosen a staging approach and set up your hardware, install Windows Server 2003 (or Windows 2000 Server) and Active Directory on your staging servers in preparation for synchronizing the configuration of production and staging environments. In most cases, you should ensure that the staging environment is running at the same operating system, service pack and hot fix levels as your production environment. This is important to ensure consistent test results. In addition, ensure that the supporting infrastructure, such as Directory Name Service (DNS), Distributed File System (DFS), and related services are also configured as in the production environment. DNS especially is critical to proper processing of GPOs. If you decide to use a staging approach that places a staging domain in your production forest, then you can use your existing production DNS infrastructure for name services.



Important

You can use GPMC to manage both Windows Server 2003 and Windows 2000 Active Directory–based domains, but you must run GPMC on a computer running a member of the Windows Server 2003 family operating system or Windows XP Professional SP1 and the .Net Framework.

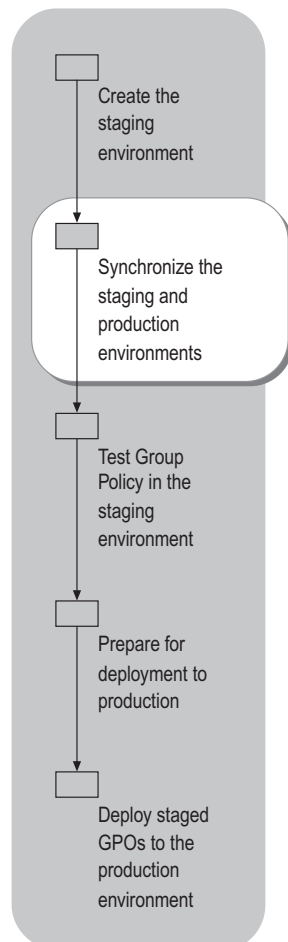
If you build a separate forest for staging, then you need to address the issue of name services integration. Name services might include either DNS or Windows Internet Name Service (WINS), depending on the types of trusts you created. You might need to create a separate DNS infrastructure for your staging environment. This is particularly true if you are using Active Directory–integrated DNS in your production forest, because Active Directory–integrated zones cannot support dynamic registration of clients from foreign forests. If you plan to create trusts between your staging and production forests, the name services infrastructure in each forest must be aware of the other. Note that if both your staging and production forests are running at Windows Server 2003 forest functionality level, and you want to create inter-forest trusts between the two forests, then DNS integration is required. However, if you are running at Windows 2000 forest functionality level, which requires the use of down-level trusts, you must have the WINS service available and integrated between the two forests to create the required trusts.

Once your staging environment is fully configured with the base elements required to deploy Group Policy, the next step is to synchronize the staging and production environments.

Synchronizing the Staging and Production Environments

Once you have created a basic staging infrastructure that reflects your production environment, you need to ensure that all GPO settings and security are identical between the two environments. Synchronization also requires ensuring that a sufficient representation of OUs, users, computers and groups exist in both environments, because you need to be able to test GPO links and the effects of security group filtering as they would exist in the production environment. Figure 3.6 illustrates the synchronization step in the staging process.

Figure 3.6 Synchronizing the Staging and Production Environments



The goal of any test environment is to ensure that it mirrors the production environment as closely as possible. You can use GPMC tools to help both with the initial synchronization and to keep the test environment synchronized with the production environment over time. The first set of tools you will use are two Windows Script Host (WSH) scripts that are installed with GPMC. These two scripts, `CreateXMLFromEnvironment.wsf` and `CreateEnvironmentFromXML.wsf`, are installed in the Scripts folder in the folder `Program Files\GPMC\Scripts`. The script `CreateXMLFromEnvironment.wsf` is run against a production domain, stores all policy-related information in an XML format file, and creates backups of the GPOs it finds in the production domain. Note that this script works only against a single domain at a time, not against an entire forest. The script `CreateEnvironmentFromXML.wsf`, uses the XML format file and any backup GPOs created by `CreateXMLFromEnvironment.wsf` to re-create GPOs and other objects from the production domain in a staging domain. Table 3.2 describes the objects and settings that `CreateXMLFromEnvironment.wsf` captures, and shows additional objects you can capture by using command-line options when running the script.

Table 3.2 Objects Captured by `CreateXMLFromEnvironment.wsf`

Object Type	Captured by Script	Additional Command-line options
All GPOs and GPO settings for the domain or OU	Yes	To get GPO settings, you must provide a Template Path by using the <code>/TemplatePath</code> option to specify a file system location to store backed up GPOs. If no template path is specified, GPOs are not backed up. You can exclude permissions on GPOs by using the <code>/ExcludePermissions</code> option.
Organizational Units	Yes	You can capture only a portion of the OU tree by using the <code>/StartingOU</code> switch, along with the DN-style path to an OU.
GPO Links and link attributes (for example, disabled, block inheritance)	Yes, except that links on site objects are not captured	None
Policy-related Permissions	Yes	You can exclude permissions by using the <code>/ExcludePermissions</code> option.
WMI Filters	Yes	None
Users	Optional	User accounts are not captured unless you use the <code>/IncludeUsers</code> option.
Security Groups	Yes	By default, only security groups defined in OUs are captured by the script. You can extend this to include all groups in the Users container and in the domain root by using the <code>/IncludeAllGroups</code> option.
Computers	No	None
Sites	No	None

There are a few things to bear in mind when using the script `CreateXMLFromEnvironment.wsf`. First, if you use the `/IncludeUsers` option to capture user objects, when those objects are re-created in the staging domain, you will need to supply a password for each user captured. You can do this by manually editing the resulting XML file and adding a password for each user. (For an example of the syntax, see the file `SampleEnvironment.xml` in the `Program Files\GPMC\Scripts` folder on any computer where you have installed GPMC.) Alternatively, if you have any users that do not have passwords specified in the XML file, the `CreateEnvironment` script will prompt you to supply a password. All users that do not have passwords specified in the XML file will be created with this password. Also note that the script does not capture computers. This is because computer objects in Active Directory correspond to physical hardware resources, and those might differ between the production and staging environments. Finally, the script captures neither sites nor GPO links on sites. Because sites can span multiple domains and can have an impact on Active Directory replication, it is best to re-create these objects, and GPO links on them, manually in your staging environment.

Example: Creating an XML Format File from a Production Environment

Assume that your production domain is called `Contoso.com`, and you want to export Group Policy and related information to create a new staging domain for GPO testing. In this example, assume that you want to capture GPOs from the entire domain and include user accounts as well as groups. To export the information you need, complete the following tasks:

1. Ensure that you have sufficient permissions on the production domain to extract the necessary data. You must have the rights to read all objects that you are capturing, including GPOs, OUs, users, and groups (and their memberships).
2. Create a folder to store the XML format file that describes the information collected by the script.
3. Create a folder to store backups of the GPOs that are extracted by the script.
4. Run the script `CreateXMLFromEnvironment.wsf` from the `Scripts` folder in the GPMC installation folder. You must precede the script name with the command `cscript` if `cscript.exe` is not your default WSH engine. For this example, type the following from the command line:

```
Cscript
"%programfiles%\gpmc\scripts\CreateXmlFromEnvironment.wsf".\production.xml
/Domain:contoso.com /DC:contoso-dc1 /TemplatePath:.\GPObackups /IncludeUsers
```

This command creates the XML format file `Production.xml` in the folder where the script is run. The backed-up GPOs are created in a sub-folder of the current folder called `GPObackups`. Placing a backslash (`\`) in front of the `production.xml` and `GPObackups` paths causes the script to use a relative path, and create the XML file and backup GPO folders in the current directory from which the script is run. Using a relative path makes it easier to copy the XML and backups to different locations from which they can be restored.

The script starts its capture at the domain level, Contoso.com. You can also run the script at an OU level, in which case you would use the `/StartingOU` option in addition to the `/Domain` option. If you exclude the `/Domain` option, the current domain is assumed. The `/DC` option tells the script to use the domain controller contoso-dc1, and the `/TemplatePath` option specifies that the backups of all of the GPOs that are captured are stored in the folder GPOBackups. Finally, the `/IncludeUsers` option ensures that user accounts are captured by the script as well.



Caution

You can open and edit the XML format files produced by the script `CreateXMLFromEnvironment.wsf` in a text editor or any XML editor. Be aware, however, that XML-formatted files must adhere to a specific syntax. If you change that syntax, you might affect the ability of the script `CreateEnvironmentFromXML.wsf` to read the input file.

Once you have captured the production environment by running the script `CreateXMLFromEnvironment.wsf`, you need to run the script `CreateEnvironmentFromXML.wsf`, using the .XML format file output by `CreateXMLFromEnvironment.wsf` as input. You must run the script `CreateEnvironmentFromXML.wsf`, from within the staging domain, or you can run this script from a computer that is not in the staging domain if you already have trusts to the staging domain in place.

Importing Production GPOs into the Staging Domain

The script `CreateEnvironmentFromXML.wsf` has a number of different options that you can use to qualify the creation of GPOs in your staging environment. In the simplest form, just supply an XML format file created from the production domain to the script and optionally direct the operation of the script to a DC in your staging domain. The script creates GPOs and related objects in the staging domain that correspond to the data that was captured from the production domain. If you need to modify this process, the script provides a number of command-line options:

- **Undo.** This option removes all objects (GPOs, GPO permissions, OUs, WMI filters, users and groups) specified by the XML format file from the staging environment. This option is useful if you need to reverse changes you made to your staging domain.
- **ExcludeSettings.** This option creates GPOs in the destination domain, but with no settings. Use it when you do not actually want to import the settings in any Group Policy objects, but rather just want to create any OUs, users, and user groups that might have been captured.
- **ExcludePermissions.** This option causes the script to ignore any policy-related permissions contained in the XML format file. Instead, when the new GPOs and other objects are created in the staging environment, they are created with the default permissions.

- **MigrationTable.** This option lets you specify a .migtable file that you create using the MTE to specify mapping of security principals and UNC paths in your production environment GPO settings to the appropriate security principals and UNC paths in the staging environment.
- **ImportDefaultGPOs.** This option imports settings into the default domain policy and the default domain controllers policy if settings for these GPOs are specified in the XML file. If this option is not specified, these GPOs will not be modified.
- **CreateUsersEnabled.** This option creates user accounts as enabled instead of disabled.
- **PasswordForUsers.** This option allows you to specify the password to use for any users that do not have passwords specified in the XML file. The same password will be used for all users that do not already have passwords specified in the XML file.
- **Q.** The Q option runs the script in quiet mode, provided that all necessary parameters have been supplied on the command line. Without this option, you are warned that this script should only be used for creating staging environments, and if necessary, you will be prompted to supply a password for any users that do not have passwords defined in the XML file.

Example: Populating the Staging Domain from the XML Format File

Assume that your staging environment is the domain test.contoso.com, and is in the same forest as the production domain captured earlier in this chapter. Even if the staging domain is not in the same forest as the production domain, the steps for populating the staging domain are the same, but different mapping of security principals using migration tables might be required. To populate the staging domain, complete the following tasks:

1. Ensure that you are running the script CreateEnvironmentFromXML.wsf with sufficient permissions in the staging domain. You should run the script as a user as a member of Domain Admins or have equivalent access in the domain.
2. Ensure that you have access to the XML format file and backup GPOs that were created in the production domain by running CreateXMLFromEnvironment.wsf.

Note that when you run CreateEnvironmentFromXML.wsf, you are only referencing the XML format file (not the location of the backup GPOs) in the command-line options. That file includes the paths to the backup GPO files. Consequently, when you specify the XML file to CreateEnvironmentFromXML.wsf, the script uses any backup GPO files in the folder that was specified when the script CreateXMLFromEnvironment.wsf was run. If you ran CreateXMLFromEnvironment.wsf using the command as shown in “Example: Creating an XML Format File from a Production Environment” earlier in this chapter, then the XML file will indicate that the backups are in a sub-folder of the current folder. If you did not use a relative path when running CreateXMLFromEnvironment.wsf, there are three ways to ensure that CreateEnvironmentFromXML.wsf, can find the required files:

- Copy the specified folder structure from the location where it was created to an identical path on the local computer from which you run `CreateEnvironmentFromXML.wsf`.
 - Specify a network share rather than a local drive when you first create the XML format file (the share must be also accessible from the location where you run `CreateEnvironmentFromXML.wsf`).
 - Edit the XML format file to change the path entries to point to a different location for the backup GPO files.
3. Run `CreateEnvironmentFromXML.wsf` from the Scripts folder in the GPMC installation folder. You must precede the script name with the command `cscript` if `cscript.exe` is not your default WSH engine. For this example, type the following from the command line:

```
Cscript CreateEnvironmentFromXml.wsf /xml:c:\staging\production.xml
/Domain:test.contoso.com /DC:test-dc1
```

The script generates a warning that the script is intended for creating staging environments only, and then prompts you to enter a password for user objects. If you use the `/Q` option and supply the password using the **PasswordForUsers** option when you run this script, these messages are not presented. If you confirm that you want to proceed, the script provides status as it processes the XML file and GPOs. You can then confirm that all steps completed correctly by using the Active Directory Users and Computers MMC snap-in and GPMC to verify that users, groups, and GPOs were successfully created.

Maintaining Synchronization of Staging and Production

The scripts `CreateXMLFromEnvironment.wsf` and `CreateEnvironmentFromXML.wsf` are used to create an initial staging environment from your production environment. But maintenance of Group Policy, including testing new and changed GPOs, is ongoing; how do you keep your staging environment synchronized with the production environment on a continuing basis? These two scripts provide an all or nothing method for populating GPOs — they are not granular enough to capture and import only specific GPOs.

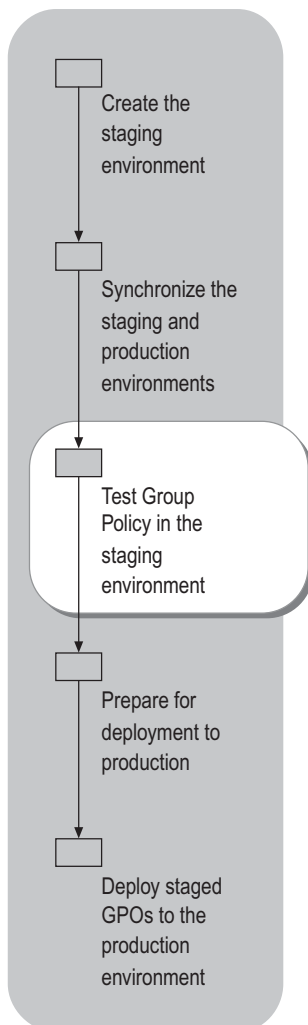
The backup and import functions in GPMC give you the ability to selectively synchronize specific GPOs between your production and staging environments. You can use the backup capability to create a backup of the settings and security of a production GPO. You can then import the backup over an existing GPO in your staging domain, thereby synchronizing it with the production GPO. For more information about backing up and importing GPOs, see “Deployment Examples” later in this chapter.

Testing Group Policy in the Staging Environment

After you have created your staging environment and synchronized Group Policy with your production environment, you can begin to test planned Group Policy changes. The best mechanism for testing Group Policy is by using a combination of the Results and Modeling tools provided with GPMC and exercising real user accounts and computers in the test environment to process actual GPOs.

The Group Policy Results tool is useful when you have applied new GPO settings to a computer and user, and need to verify that all of the expected settings were actually applied. Group Policy Modeling can be used to determine the effects of changing the location of a user or computer within the Active Directory namespace, changing the group membership of a user or computer, or to observe the effects of a slow link or loopback policy. The Group Policy Modeling tool lets you test the effects of a change without actually making the change, while Group Policy Results tool tells you what actually happened. Group Policy Results runs on the target computer, so you must have access to that computer. Group Policy Modeling runs on a Windows Server 2003 Domain Controller, so there must be one available to run the modeling process. Note that with Group Policy Modeling, you can model policy settings on computers running Windows 2000 and Windows XP Professional as well as Windows Server 2003. Bear in mind that the Group Policy Modeling tool simulates processing of policy, while the Group Policy Results tool shows the effects of policies actually processed.

Figure 3.7 illustrates this step in the process.

Figure 3.7 Testing Group Policy in the Staging Environment

Testing by Logging on as Test User

The first and best method for testing Group Policy is to make the actual changes to your staging domain GPOs and then test the results by logging on to workstations with test user accounts to observe the effect of the changes. In this way you can see first hand how the user has been affected by the changes.

Testing by Using Group Policy Results

You can use the Group Policy Results Wizard in GPMC to get detailed reports of which policies are applied to users and computers. You can then make any needed changes in your test GPOs accordingly. The Group Policy Results Wizard is used after all Group Policy is processed for a given user and computer to inform you as to what settings were applied. The results are gathered by querying the WMI-instrumented Group Policy logging facility on a Windows XP-based computer or Windows Server 2003-based server that processed Group Policy. The wizard thus returns the settings that were actually applied rather than expected settings.

For more information about the Group Policy Results Wizard, see “Deploying a Group Policy Infrastructure” in this book.

Testing by Using Group Policy Modeling

The second method for testing Group Policy is to use the Group Policy Modeling Wizard in GPMC to model changes to your environment before you actually make them. Group Policy Modeling lets you perform hypothetical tests on user and computer objects prior to a production rollout to see how Group Policy settings would be applied if you made changes such as moving the user or computer objects to a different OU, changing their security group membership, or changing the effective WMI filters. Be aware, however, that results obtained using Modeling are modeled rather than actual policy settings. Therefore, once you have modeled the scenario that meets your needs, it is always best to use the GP Results wizard to verify the expected settings.

Because Group Policy Modeling does not let you specify proposed changes to settings in a GPO, you need to make the proposed changes to your staging GPOs and then run the Group Policy Modeling Wizard for a given OU, user, or computer to determine the resultant set of policy.

Group Policy Modeling also gives you the ability to model Group Policy behavior when your computers are processing policy across a slow network link, which can affect which Group Policy extensions are processed. For example, if a computer connects to a domain controller over a slow network link (defined by default as any rate slower than 500 kilobits per second (Kbps)) then Group Policy extensions such as Software Installation and Folder Redirection are not processed. Group Policy Modeling can simulate a slow link speed and use it to determine what the effective policy settings will be for the user and computer being modeled. In addition, Group Policy Modeling supports testing the effects of Group Policy loopback processing. With loopback processing enabled, the same settings are applied to a computer regardless of the user who logs on to it. Note that you must specify that you want to model loopback processing within the Modeling wizard; loopback processing is not modeled by default.

You can specify slow-link detection, loopback processing, or both when using the Group Policy Modeling Wizard. For loopback processing, you can choose whether to replace or merge user-specific policy. The replace mode replaces all of a user's normal policy settings with those defined in the user configuration of the GPOs that apply to the computer object (the loopback settings). Merge mode merges the user's normal policy settings and the loopback settings. In the case where a policy item in the user's normal policy conflicts with the loopback settings, the loopback settings are applied.

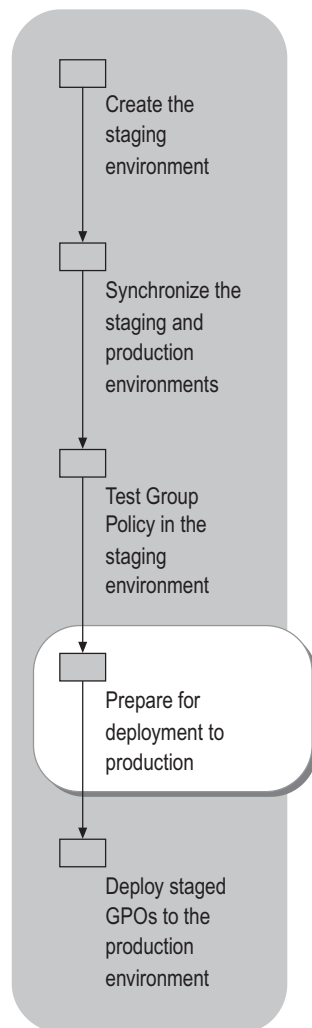
Note that the Group Policy Modeling process actually runs on a Windows Server 2003 domain controller in your Active Directory domain. By contrast, the Group Policy Results Wizard runs at the Windows XP-based workstation or Windows Server 2003-based server that is processing Group Policy. Group Policy Results uses the RSoP WMI provider to generate information about policy processing. Group Policy Modeling relies on the Windows Server 2003 Resultant Set of Policy Provider service to perform its analysis.

For more information about the Group Policy Modeling Wizard, see "Deploying a Group Policy Infrastructure" in this book.

Preparing for Deployment to Production

Once you are satisfied that your changes to Group Policy have been thoroughly tested in the staging environment, you are almost ready to deploy the new or changed GPOs in your production environment. Before you can do that, however, you need to assess whether you will need to map security principals or UNC paths contained in your GPOs to different values as part of the migration. This step is illustrated in Figure 3.8.

Figure 3.8 Preparing for Deployment to Production



Determining Your Migration Mapping Requirements

Your staging environment might be a test domain in production, a separate but trusted test forest, or a separate test forest that is not trusted. In each case, you will probably have to create and use a migration table as you deploy new or changed GPOs in your production environment. Migration tables satisfy three different types of mapping requirements:

- You need to map an Access Control Entry (ACE) on one or more GPOs to different security principals as you migrate the GPOs to the production environment. The ACEs on a GPO describe which users, computers and computer groups will process that GPO, and which users or user groups can view and edit settings in or delete the GPO.
- You need to map security principals within security policy settings or Folder Redirection settings defined in one or more GPOs. Specifically, policies such as User Rights Assignment, Restricted Groups, File System, Registry, or System Services allow you to specify particular users or groups who can access or configure those resources. The Security Identifier (SID) for that user or group is stored in the GPO and must be modified to reflect production domain users or groups when the GPO is migrated.
- You need to map UNC paths when you have defined software installation policy, folder redirection or scripts policies that reference UNC paths. For example, you might have a GPO that references a script stored in an external path, such as the Netlogon share on a remote server. This path might need to be mapped to a different path when the GPO is migrated. UNC paths are usually specific to a given environment, and might need to be changed when you migrate the GPO to your production environment.

If any of these three conditions above is true, you will need to create a migration table that can be used to map the values in your test GPOs to the correct values in the production domain when they are migrated

Creating Migration Tables

Migration tables are XML format files that specify how to map security principals and UNC paths to their production domain equivalents. Migration table files have a default file name extension of .migtable. The Migration Table Editor (MTE) is a GPMC tool that can be used to create and edit migration tables. It can be accessed in either of two ways:

- You can start MTE and create or edit a migration table during a GPMC copy or import operation. In this case, MTE starts in a separate window that allows you to create a new migration table or edit an existing one.
- You can start MTE in stand-alone mode (independently of an import or copy operation) and create or edit the migration table in advance of migrating GPOs to your production environment.

You can also create migration tables by using a supplied script, as described later in this section.

An advantage of creating the migration table in advance is that you can be sure that the migration settings you define are exactly what you want before beginning the deployment. Therefore, when you are ready to move your test GPOs into production, you should first create one or more migration tables for the GPO(s) that you need to migrate. Note that a single migration table can be used for more than one GPO. You might use a single migration table that covers every possible security principal and UNC path combination for a given migration from a staging-to-a production domain. In that case you can simply apply the same migration table to every GPO that is deployed from the staging domain to the production domain, and those principals and paths that match will be correctly mapped.

Using the Stand-alone Migration Table Editor

To start MTE in stand-alone mode, run Mtedit.exe from the GPMC installation folder. MTE starts with a blank migration table that you can populate manually by typing entries into the grid, or you can auto-populate the table by using one of the auto-populate methods.

Auto-populating the migration table

The easiest way to start creating a migration table is to use one of the auto-populate features, accessed from the **Tools** menu in MTE. You can auto-populate from both backup GPOs and from live GPOs. To auto-populate a migration table, you need to perform the following tasks:

1. Choose to auto-populate the table from live GPOs or from backup GPOs.

When you are ready to migrate a GPO in your staging environment into your production environment, you can use **Populate From GPO** against the live GPO in the staging environment to start the migration table. The process for auto-populating the table from a backup GPO is the same, except that you must provide a path to the backup GPO. In that case, if you have more than one backed up GPO, a list is displayed from which you can choose.

Note that you can select multiple GPOs or backup GPOs when auto-populating a single migration table. This allows you to use a single migration table for all GPOs in a domain.

2. Choose whether to include security principals from the DACL on the GPO.

When you auto-populate a migration table, you can select the option to include security principals from the DACL on the GPO. If you select this option, security principals on the GPO's DACL are included in the table along with security principals referenced in the GPO settings. Duplicate source security principals are not repeated in the migration table. MTE supports a number of different object types that can be mapped, as described in Table 3.3.

Table 3.3 Object Types Supported in the Migration Table

Object Type	Used to Map...
User	Individual user accounts.
Domain Global Group	Domain global groups.
Domain Local Group	Domain local groups.
Universal Group	Universal groups.
Computer	Computer names. For example, an individual computer can be given read and apply Group Policy permissions on a GPO.
UNC Path	UNC paths used in software installation policy.
Free Text or SID	<p>Undetermined security principals. For example, you might reference security principals in a GPO by name rather than by SID (typed as "administrators" instead of "DomainX\Administrators"); or it might not be possible to resolve security principals to determine the type.</p> <p>This can occur because, for example, when setting restricted group security policy, you can type in the name of the group rather than resolve it against a live domain. In this case, the group name is stored in the Group Policy object as its name rather than its corresponding SID. MTE considers such a security principal as Free Text or SID.</p> <p>In addition, you can type raw SIDs into the MTE. In that case, because the object type is not known by MTE, it must be specified as Free Text or SID.</p>

3. Modify the **Destination Name** for each security principal and UNC path.

After you have populated the migration table, you can choose to modify the **Destination Name** field for each record. The default **Destination Name** value is **Same As Source**, which means that the same security principal or UNC path will be used in the destination GPO as the source. In this case, the value is copied without modification and the mapping accomplishes no changes. Typically you will need to change this field for one or more source entries when deploying a GPO from a test to a production environment. To change the destination field, you can either type in an entry or right-click the field and make a choice from the menu.

The two menu options available are **Browse** and **Set Destination**. Choosing **Browse** allows you to use the object picker to select a security principal in any trusted domain. If you choose **Set Destination**, you can choose one of three options:

- **No Destination.** If you specify **No Destination**, the security principal is not included in the destination GPO when migrated. This option is not available for UNC path entries.
- **Map by Relative Name.** If you specify **Map by Relative Name**, the security principal name is assumed to already exist in the destination domain, and that destination name will be used for the mapping. For example, if the source name is **Domain Admins** for the test.contoso.com domain and you are migrating the GPO into the contoso.com domain, then the name Domain Admins@test.contoso.com will be mapped to Domain Admins@contoso.com. The group must already exist in the target domain for the actual import or copy operation to succeed. This option is not available for UNC path entries.
- **Same As Source.** If you specify **Same As Source**, the same security principal is used in both the source and destination GPOs. Essentially, the security entry is left as-is. Note that this option is only practical if you are migrating from a test domain in the same forest as the production domain, or if you are migrating from a test domain in a different forest that trusts the production forest. The requirement for a source name to map successfully is that it can be resolved by users and computers in the production forest.

There are some restrictions on the options available for the destination name. UNC paths only support the **Same As Source** option, or you can manually enter a different UNC path. Security Principals designated as Free Text or SID do not support **Map by Relative Name**.

It is also important to note that you will receive a warning if you map from one group type to another. For example, if you have a source principal that is a Domain Global Group and you select a Domain Local Group as the destination, you will be warned that the destination name is of a different type from the source. If you then try to validate the file, the validation process fails, but you can still use the migration table to perform a migration. Note that the migration table does not support mapping to a built-in security group such as the Administrators group.

If you need to delete a row from MTE, select the desired row, then right-click the row and choose **Delete** from the menu.

4. Validate the migration table.

Before saving the migration table, it is best to validate the file. To do this, from the **Tools** menu, choose **Validate**. The validation process determines if the XML format of the resulting file is valid and verifies that the destination names are valid from a migration perspective. For example, if you enter a UNC path for the destination, and the path does not exist, the validation process will return a warning. Specifically, the validation process:

- Validates the existence of destination security principals and UNC paths.
- Checks that source entries with UNC paths do not have destinations of Map By Relative Name or No Destination, which are not supported.
- Checks that the type of each destination entry in the table matches the real type in Active Directory.

If you are entering data manually, the validation process is especially important to ensure that an entry error does not prevent a successful migration. Note that a validation of the mapping file might fail because the user editing the file does not have the ability to resolve the security principals or UNC paths specified in the file. However, that does not mean that the file will not work as expected during a migration, provided that the user who performs the migration can resolve the security principal and UNC names. Validation messages will indicate whether there is a syntax error in the table or whether the validator simply cannot resolve a security principal name or UNC path. In the case of a name resolution failure, ensure that you will have sufficient access to both source and destination resources during the actual migration.

5. When you are finished editing the table, save the resulting .migtable file by choosing **Save** from the **File** menu.

Entering Migration Table Entries Manually

If you choose not to use the Auto-Populate feature, or if you need to enter some data manually, take care to adhere to the proper formats in order for the migration table to be valid. Table 3.4 shows the proper form for each object type supported in the migration table. Note that these formats are required in both source and destination fields.

Table 3.4 Required Formats for Migration Objects

Object Type	Required Format
User	<p><i>a. UPN - User@UPN suffix</i> <i>b. SAM – NetBIOS domain name\user</i> <i>c. DNS – DNS domain name\user</i> For example, PilarA@contoso.com, contoso\PilarA, or contoso.com\PilarA.</p>
Domain Global Group	<p><i>a. UPN - Group@UPN suffix</i> <i>b. SAM – NetBIOS domain name\group</i> <i>c. DNS – DNS domain name\group</i> For example, Domain Admins@contoso.com, contoso\Domain Admins or Contonso.com\Domain Admins.</p>
Domain Local Group	<p><i>a. UPN - Group@UPN suffix</i> <i>b. SAM – NetBIOS domain name\group</i> <i>c. DNS – DNS domain name\group</i> For example, Administrators@contoso.com, contoso\Administrators, Contoso.com\Administrators.</p>
Universal Group	<p><i>a. UPN - Group@UPN suffix</i> <i>b. SAM – NetBIOS domain name\group</i> <i>c. DNS – DNS domain name\group</i> For example, Enterprise Admins@contoso.com, contoso\Enterprise Admins, or contoso.com\Enterprise Admins.</p>
Computer	<p><i>a. UPN – Computer Name\$r@UPN suffix</i> <i>b. SAM – NetBIOS domain name\computer name\$</i> <i>c. DNS – DNS domain name\Computer name\$</i> For example, server1\$@contoso.com, contoso\server1\$, or contoso.com\server1\$. The \$ indicates the computer's hidden computer account.</p>
UNC Path	\\servername\sharename\ For example, \\server1\packages.
Free Text or SID	Either a string or the string representation of a SID. For example, "PilarA" or "S-1-5-21-1473733259-1489586486-3363071491-1005". SIDs cannot be specified in the destination field.

Creating a Migration Table by Using a Script

If you need to automate the process of creating migration tables, you can use a supplied script, `CreateMigrationTable.wsf`. You can also use this script in place of MTE to generate the initial migration table, and then use MTE to modify the table. The script `CreateMigrationTable.wsf` is located in the Scripts folder in the GPMC installation folder. The script supports auto-populating a migration table using either a live GPO or a backup GPO location. You can also have the script read from all GPOs within a domain. In that case, all possible security principals found in GPOs in the staging domain are put into the migration table, and that single migration table can be used for any GPO deployment from that staging domain to a production domain.

To use the script `CreateMigrationTable.wsf`, from the command line, change directories to the Scripts folder and run the script, preceded by the `Cscript.exe` command. Note that the script always includes the security principals that are part of the DACL on the GPO, unlike MTE, which gives you the option to include them. The script also has an option to set the destination name to **Map by Relative Name** rather than the default **Same As Source**. You use the `/MapByName` argument to implement relative naming. The following command illustrates how the script can be used. In this command, a GPO named Finance OU Desktop Policy is located in a staging domain named `staging.contoso.com`. This command auto-populates the migration table called `FinanceStaging.migtable` from the live GPO:

```
Cscript.exe CreateMigrationTable.wsf c:\migtables\FinanceStaging.migtable /GPO:
"Finance OU Desktop Policy" /domain:staging.contoso.com
```

To create a migration table from the backup of this GPO instead of from the live copy, simply add the `/BackupLocation` option to the command above, and provide a folder path that contains the backup copy of the GPO. Note that if you use the `/BackupLocation` option and there is more than one backup GPO located in that folder path, all available backed up GPOs will be used to populate the migration table.

Final Preparations for Deployment

As a final step before your production deployment, you should back up your staging GPOs. A backup is required if you are using a GPO import to perform your migration from staging to production. This method is required in cases where your staging environment is in a forest that is separate from and not trusted by your production domain, or where you need to update an existing GPO that already exists in your production environment. You can use GPMC to back up one or more GPOs or, you can use the script `BackupGPO.wsf` to back up a single GPO, or use the script `BackupAllGPOs.wsf` to back up all GPOs in the staging domain. To back up a GPO by using GPMC, in the console tree, right-click the GPO and select **Backup** from the menu.

To back up a GPO by using `BackupGPO.wsf`, run the script from the Scripts folder in the GPMC installation folder. The following command-line syntax backs up the GPO Finance OU Workstation Security Policy in the domain `staging.contoso.com` to the folder `c:\gpobacks`:

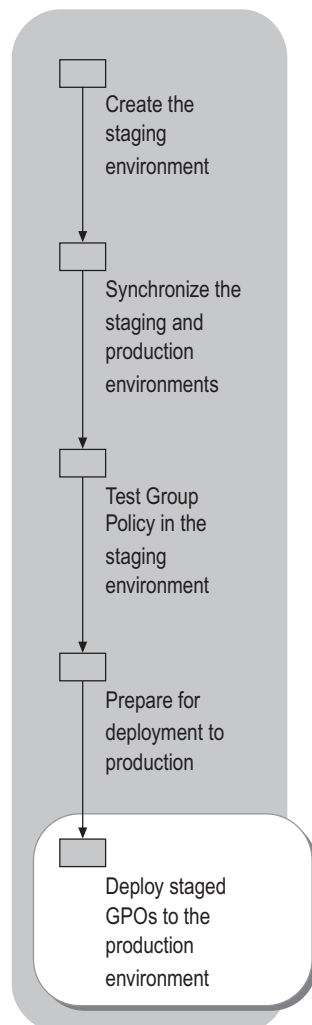
```
Cscript.exe backupgpo.wsf "Finance OU Workstation Security Policy" c:\gpobacks
/comment:"Backup prior to prod" /domain:staging.contoso.com
```

The preceding syntax includes a comment that indicates the purpose of the backup.

Deploying Staged GPOs to the Production Environment

Once you have built your staging environment, synchronized it to your production environment, tested new and changed GPOs, and created migration tables, you are ready to perform the actual production deployment. Figure 3.9 shows this final step in the process.

Figure 3.9 Deploying Staged GPOs to the Production Environment



Deployment Precautions

To ensure uninterrupted service to your users, it is a good idea to observe some precautions when migrating staged GPOs to your production environment. Although migrating new GPOs is typically a quick process that does not adversely impact production users or computers, it is prudent to avoid making such a change until the least possible number of users will be affected. Typically this might be during off hours, when users are not active on the network.

Remember that when a GPO is updated, the update is performed first against the Domain Controller that is currently targeted by GPMC for a particular domain. If you are using GPMC to perform the migration, you can click the **Domains** item in the console tree to see which DC is currently being used for each domain under management. To change the DC, right-click the domain name and choose the **Change Domain Controller** from the menu before migrating your changes.

GPO Replication

Keep in mind that GPO changes propagate according to your Active Directory replication and Sysvol File Replication service topologies, and therefore might take an extended period of time to replicate to all locations in a worldwide Active Directory deployment. Also keep in mind that a GPO is composed of two parts — the portion that is stored and replicates as part of Active Directory, and the portion that is stored and replicates as part of Sysvol. Because these are two separate objects that need to replicate across your network, both need to be synchronized before the new GPO is applied.

You can view the replication status on a given DC by using GPMC. From the Group Policy Objects node in GPMC, click a GPO to check, and then select the **Details** tab in the details pane. If the GPO is synchronized on that DC, the Active Directory and Sysvol version numbers will be identical for user and computer configuration. However, the user version numbers do not need to match the computer version numbers.

Requirements for Performing the Deployment

The primary requirement to keep in mind as you prepare to deploy your staged GPOs to your production environment is whether you have sufficient permissions on the destination GPOs. You typically need only read access to the source domain to complete a deployment. Depending on the configuration of your staging environment, you might need to take some specific steps prior to migration. If you are performing a copy operation, you will need to have sufficient permissions to create a new GPO in the destination domain. If you are importing a backup GPO, you will need to be able to read the backup files, wherever they might be located, and then have sufficient permissions to modify an existing GPO in the destination domain that is the target of the import operation. Finally, you should ensure that the migration table that you created for each GPO that requires one is stored where it is accessible to you while performing the migration. The following checklist summarizes the items to verify before running the migration:

- **For a copy operation:** ensure that the destination domain is trusted by the source domain and that you have GPO Creation permissions on the destination domain.
You can confirm GPO Create permissions on a domain by using GPMC. Click the **Group Policy Objects** node and, in the details pane, select the **Delegation** tab to see which users or groups can create new GPOs in the domain.
- **For an import operation:** ensure that you have access to the backup GPO files and that you have GPO Edit Settings permission on the destination GPO.
- **If you are using a migration table (.migtable):** ensure that you have access to the file from GPMC.

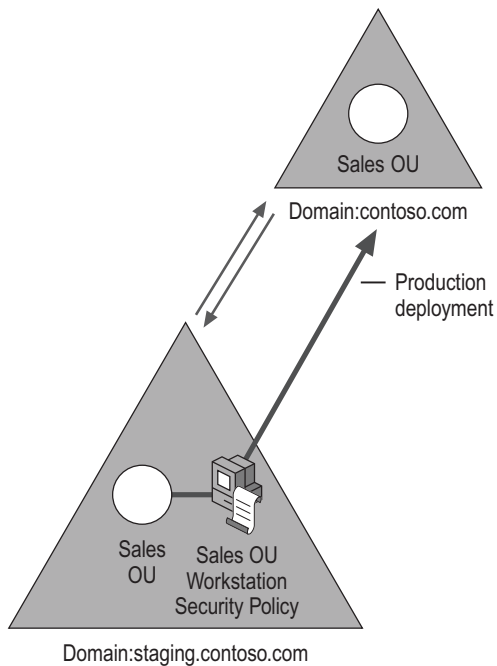
Deployment Examples

The following two examples illustrate deploying GPOs from staging to production environments. In the first example, the staging domain is located in the same forest as the production domain. In the second example, the staging domain is in a separate forest that is not trusted by the production domain. If you use a separate staging forest that is trusted by the production domain, the steps are the same as in the first example, where the staging domain is part of the production forest.

Staging to a Production Domain in a Single Forest or from a Trusted Staging Forest

When the staging domain is part of your production forest or you have a separate staging forest that is trusted by your production domain, your deployment method depends on whether the GPO is new or changed. If the GPO is new and does not exist in the production domain, use the copy method to deploy the new GPO. If you are deploying an update to an existing GPO, then you must use the import method to update the production GPO's settings with those from the backup staging GPO.

In this example, you will deploy a new GPO named **Sales OU Workstation Security Policy** from the staging domain to the production domain by using GPMC. Figure 3.10 illustrates the staging and production domain configuration and shows the accompanying migration table.

Figure 3.10 Migration from Staging to Production Domain

Migration Table Editor - E:\migtables\to-prod-mapping.migtable		
File Edit Tools Help		
Source Name	Source Type	Destination Name
Sales Admins@staging.contoso.com	Domain Global Group	Sales Admins@contoso.com
Authenticated Users	Unknown Group	<Same As Source>
WORKSTATION1\$@staging.contoso.com	Computer	<None>
Domain Admins@staging.contoso.com	Domain Global Group	<Map by Relative name>
Administrators	Unknown Group	<Same As Source>
Enterprise Admins@staging.contoso.com	Domain Global Group	<Map by Relative name>
► Sales Users@staging.contoso.com	Domain Global Group	Sales Users@contoso.com
sales users	Unknown Group	Sales Users@contoso.com
\\server1\packages	UNC Path	\\prodserver\packages
*		

Before beginning the deployment load both the source and destination domains in GPMC. If you are copying from a separate trusted forest, open both forests in GPMC.

► **To deploy a new GPO using the copy method**

1. In GPMC, in the staging domain, right-click the GPO that you plan to migrate and choose **Copy** from the menu.
2. In GPMC, in the production domain, right-click **Group Policy Objects** and choose **Paste** from the menu or drag-and-drop the source GPO onto the Group Policy Objects node of the destination domain. The Cross-Domain Copying Wizard starts.
3. On the **Cross-Domain Copying Wizard** page, click **Next**, select the option to Preserve or migrate the permissions from the original GPOs, and then click **Next**.

If you choose the first option, **Use the default permissions for new GPOs**, this GPO will receive the default permissions that would be applied to any new GPO in the production domain. For this example, you want to use the second option, **Preserve or migrate the permissions from the original GPOs**, because that option lets you use a migration table to map the DACL on the staging GPO to its production equivalents.

The wizard scans the source GPO to determine any security principal or UNC path mapping requirements. After these are found you can advance the wizard to the next step.

4. On the **Migrating References** page of the **Cross-Domain Copying Wizard**, select the option to either copy the security principals exactly as they exist in the source GPO to the destination or to use a migration table to map references and click **Next**.

The wizard gives you two choices for performing the migration. The first choice, **Copying them identically from the source**, leaves all security principals and UNC paths in the new GPO exactly as they are in the source. Because you are migrating a new GPO from the staging environment to the production environment, you need to choose **Using this migration table to map them to new values in the new GPOs** instead. This option lets you choose a migration table to use as part of the deployment. You further have the option to **Use migration table exclusively...** If you check this option the wizard will attempt to map all security principals and UNC paths using the migration table you specify. If a security principal or UNC path that exists in the source GPO is not present in the migration table, then the entire migration fails. This is useful to ensure you have accounted for all security principals and UNC paths in your migration table. After you make your choice move to the next step in the wizard, which is the summary screen prior to migration.

5. On the **Completing the Cross-Domain Copying Wizard** page, you can see your chosen migrations options prior to performing the actual migration. This page shows the source GPO you have chosen, the option you chose for migrating permissions and the migration table (if any) that you will be using. If you need to change an option, you can select **Back** to go back through the wizard and change your choices.
6. When you click **Finish**, the migration of the staging GPO begins. Keep in mind that the new GPO is being created in the production domain but will not yet be linked to any container objects.
7. When the wizard completes the copy operation, right-click the Active Directory site, domain, or OU to which you want to link the copied GPO, and then select **Link an Existing GPO** from the menu. In the **Select GPO** dialog box, select the GPO you just copied.

After you link the new GPO, and replication is complete, the GPO is live in the production domain.

Using a Script to Perform a Copy Deployment

You can also perform a copy deployment by using the script CopyGPO.wsf, which is installed in the Scripts folder in the GPMC installation folder. This script copies a GPO between staging and production domains in a single command. To perform the same copy operation as in the foregoing procedure, use the following command:

```
Cscript CopyGPO.wsf "Sales OU Workstation Security Policy" "Sales OU Workstation
Security Policy" /SourceDomain:staging.contoso.com /TargetDomain:contoso.com
/SourceDC:staging-dc1 /TargetDC:prod-DC1
/migrationtable:c:\migtables\SalestoProd.migtable /CopyACL
```

The first two arguments in this command specify the same name for both the source and target GPO. The next four arguments specify the source and target domain names and a domain controller in each domain. The /migrationtable argument specifies the migration table to use and the /CopyACL argument is used to preserve the DACL from the source GPO and use the specified migration table to map the source DACLs to their production domain equivalents.

Deploying to a Production Domain from an Untrusted Staging Forest

If you are deploying a GPO from a staging forest that is not trusted by the production forest, the only choice for deployment is an import operation. You can also use an import to deploy an update to an existing GPO in the production domain even if a trust relationship exists between the staging and production domains.

Import Operation Prerequisites

Before performing the deployment in this example, there are some prerequisites that you should be aware of:

- If you are deploying a new GPO by using GPMC, you need to create a new, empty GPO in your production domain that can act as a target for the import operation. Remember that the GPMC import operation works by importing the settings from a backup GPO into an existing destination GPO. However, you can also use the script `ImportGPO.wsf` to create a new GPO automatically, as part of the import process.
- Before beginning the import, make sure you back up the GPOs from your staging domain that you plan to deploy to production. This is necessary because the import operation uses backup GPOs rather than live GPOs.
- If you are using the GPMC UI rather than a script to perform the import, you have the opportunity to back up the current production GPO before completing the import. You should always back up an existing production GPO before deploying a new version in case there are problems with the deployment. In that event, you can perform a restore operation from GPMC to restore the previous version of the GPO.

When these prerequisites have been satisfied, you are ready to deploy a new GPO into the production environment using the import method.

► To deploy a new GPO to the production domain using the Import method

1. In GPMC, in the production domain, right-click the GPO to be updated and select **Import Settings** from the menu.

The Import Settings Wizard starts.

2. In the **Import Settings Wizard** on the **Backup GPO** page, select **Backup** to back up the existing production GPO prior to performing the import, and then click **Next**. When you select the **Backup** button, you're given the option of choosing a location to store your backup and a name to reference it by. Select the **Backup** button to start the backup process.

Once the wizard finishes backing up your production GPO, from the **Backup location** page, you need to choose the folder that contains the backup of the staging GPO that you want to import. You must have access to the folder where you backed up your staging GPOs. If your backups were made on a server in your staging forest, you might need to map a drive to that folder from the workstation where you are running the import operation, using credentials from the staging forest.

3. After you select the backup folder, choose **Next** to present the **Source GPO** page. This page presents a the list of backup GPOs, from which you can choose the staging GPO you want to import. Once you make the choice, click **Next**.

4. On the **Migrating References** page, you will see the same options for migrating security principals as in the **Cross-Domain Copying Wizard** used in the previous copy method. You can choose to either use the existing security principal information contained in the staging GPO or apply a migration table against it. Because you are deploying a GPO from staging domain that does not have a trust relationship with the production domain, you must use a migration table to migrate security principal and UNC path information. Otherwise, the security principals and UNC paths referenced in the untrusted forest cannot be resolved by the production domain. To select a migration table to use, choose the **Using this migration table to map them in the destination GPO** option and then select a path to the migration table you created for this migration. You can select the **Use migration table exclusively...** option to only import the GPO if all security principals found in the backed up version are accounted for in the migration table.
5. Select **Next** to view the **Completing the Import Settings Wizard** page which presents a summary of your chosen migration options. You can select **Back** if you need to go back to change some of the options prior to the import. Select **Finish** to start the import operation.

If you created the production GPO from scratch to perform this import, you will need to link the new GPO to the appropriate container object. To link the GPO, in GPMC, in the production domain, right click the Active Directory site, domain, or OU to which you want to link the imported GPO and choose Link an Existing GPO from the menu. Once you link the new GPO and replication is complete, the GPO is live in the production domain.

Using a Script to Perform an Import Deployment

You can also perform an import deployment by using the script ImportGPO.wsf, which is installed in the Scripts folder in the GPMC installation folder. This script lets you import a backup GPO into your production domain. If the target GPO does not yet exist, the script also lets you create a new GPO to receive the import as part of the process. To perform the same import operation as described in the previous procedure, type the following command:

```
Cscript ImportGPO.wsf c:\gpobacks "Sales OU Workstation Security Policy" "Sales OU
Workstation Security Policy" /CreateIfNeeded
/MigrationTable:c:\migtables\salesprod.migtable /Domain:contoso.com
```

The first argument in this command specifies the location of the backup GPO files. The second argument specifies the name of the backed up GPO to import from (you can instead provide the Backup ID, which is a 128-bit GUID value generated by the backup utility to uniquely identify the backup). The third argument specifies the name of the destination GPO to import into. The /CreateIfNeeded argument indicates that if the destination GPO does not yet exist, it should be created before performing the import. The /MigrationTable argument specifies the path and name of the migration table file. The /Domain argument provides the DNS name of the destination domain.

Rollback

In the event that you have a problem with a GPO after you deploy it from the staging environment to the production environment, the best way to roll back the deployment is to use the backup GPO you created in the previous deployment steps to restore the original GPO. You can also use the `RestoreGPO.wsf` script to perform the restore process. As part of your deployment, it is a good idea to create a set of scripts that can perform an automated rollback of all of your changes using `RestoreGPO.wsf`. In the event that you need to perform a rollback, the script is ready and available to use with minimal user disruption.

Additional Resources

These resources contain additional information related to this chapter.

Related Information

- “Deploying a Group Policy Infrastructure” in this book for detailed information about Group Policy and GPMC features and capabilities.
- “Planning a Managed Environment” in this book for more detailed information about using IntelliMirror to create a managed environment.

Related Help Topics

For best results in identifying Help topics by title, in Help and Support Center, under the **Search** box, click **Set search options**. Under **Help Topics**, click to select the **Search in title only** check box.

- “Group Policy” in Help and Support Center for Windows Server 2003.
- Help in GPMC for detailed information about using GPMC to help deploy Group Policy and troubleshoot your deployment.

Deploying Security Policy

4

Administrators who deploy enterprise networks must design and implement many aspects of security. As part of your security strategy to manage servers and workstations, you can deploy Group Policy with the Active Directory® directory service to specify options for Internet Protocol security (IPSec), security settings, software restrictions policies, and wireless network policies.

In This Chapter

Overview of Security Policy Deployment	158
Designing Security Policy	162
Configuring Security Policy	181
Additional Resources	194

Related Information

- For more information about security in the Microsoft® Windows® Server 2003 operating systems, see the security chapters in *Designing and Deploying Directory and Security Services* of this kit.
- For more information about Internet Authentication Service (IAS) and wireless networks, see “Deploying IAS” and “Deploying a Wireless LAN” in *Deploying Network Services* of this kit.
- For more information about IPSec, see “Deploying IPSec” in *Deploying Network Services* of this kit and the *Networking Guide* of the *Microsoft® Windows® Server 2003 Resource Kit* (or see the Networking Guide on the Web at <http://www.microsoft.com/reskit>).

Overview of Security Policy Deployment

Your organization's data is subject to various types of risks, including user errors and malicious attacks. Attackers can gain access to the system, rendering systems useless or disrupting services. Attackers can also modify, delete, or steal information. As you analyze the potential security threats and how to handle those threats, consider how much time, money, and effort you want to invest in developing security strategies and controls for your organization.

Group Policy is one of the main tools that you can use to specify security policy for servers, workstations, and domain controllers. By using Group Policy, you can create and apply security policies to simplify and centralize the process for configuring and managing security for servers running Microsoft® Windows® 2000 Server and Windows Server 2003 and workstations running Microsoft® Windows® XP Professional and Microsoft® Windows® 2000 Professional.

You can use Group Policy to specify configuration options for IPSec, security settings (such as user rights, password policies, file and registry access control lists [ACLs], and service startup modes), software restriction policies, and wireless network configurations.

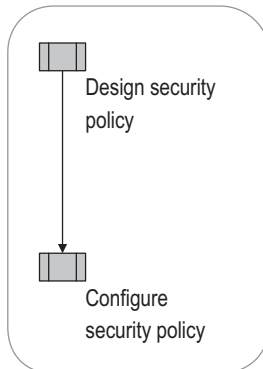
Before you deploy security policies by using Group Policy in an Active Directory environment, you must complete your deployment design for the following areas:

- **IT requirements.** Understand how domains and organizational units (OUs) are created and managed in your organization and obtain a list of the administrative owners.
- **Active Directory and security.** You must have Active Directory to use Group Policy. While you are deploying Active Directory, design the OUs in your organization to delegate administration authority and to implement Group Policy. Create a security plan that includes authentication, password requirements, resource security (such as file security), auditing, and security group membership. For more information about Active Directory and creating a security plan, see *Designing and Deploying Directory and Security Services* of this kit.

Security Policy Deployment Process

To provide security for their organizations, administrators must plan and develop a strategy that protects the availability, integrity, and confidentiality of the organization's data. Implementing security settings by using Group Policy ensures that any changes that you make to a Group Policy object (GPO) setting affects all servers and workstations in the OU or domain to which the GPO is linked.

Figure 4.1 Planning a Security Strategy



Security Policy Concepts

Group Policy is the infrastructure in Active Directory that enables centralized management of user and computer settings. Use Group Policy to define security configurations for groups of users and computers, including the following security settings:

- Account policies (password policy, account lockout policy, and Kerberos policy)
- Local policies (user rights assignment, audit policy, and security options)
- IPSec policies
- Software restriction policies
- Wireless network configurations
- File and registry ACLs
- Service startup modes
- Public key policies

For more information about individual security policies, see “Security Settings” in Help and Support Center for Windows Server 2003.

The Group Policy settings that you create are contained in a GPO. By associating a GPO with selected Active Directory system containers — sites, domains, and OUs — you can apply the GPO’s policy settings to the users and computers in the Active Directory containers. Although some security settings affect user accounts, most settings are controlled by computer settings that must be applied to computers accounts; only software restriction policies and public key policies can be applied to user accounts.

For more information about Group Policy design, see “Designing a Group Policy Infrastructure” in this book. For information about the mechanics of Group Policy, see the *Distributed Services Guide* of the *Windows Server 2003 Resource Kit* (or see the Distributed Services Guide on the Web at <http://www.microsoft.com/reskit>).

Group Policy Management Console

The Group Policy Management Console (GPMC) is a tool that permits you to manage Group Policy for multiple domains and sites in one or more forests. This chapter assumes that you are using GPMC for security policy deployment and management.

GPMC is not included with Windows Server 2003. To obtain GPMC, see the Group Policy Management Console (GPMC) link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Starting GPMC

To start GPMC, click **Start**, click **Programs**, click **Administrative Tools**, and then click **Group Policy Management**. GPMC can be used on computers that are running Windows XP Professional and Windows Server 2003. The procedures in this chapter use GPMC.

For more information about using GPMC, see Group Policy Management Console Help. To view GPMC Help, open GPMC, right-click **Group Policy Management**, and then click **Help**.

Security Configuration Manager

Windows 2000 and Windows Server 2003 provide an extensive set of security technologies and management tools, including the Security Configuration Manager tools, support for IPSec, the Kerberos V5 authentication protocol, public key infrastructure (PKI), Encrypting File System (EFS), and smart cards.

The Security Configuration Manager is a set of tools that includes:

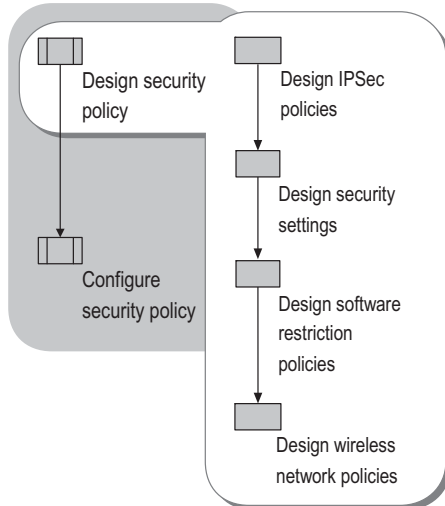
- **Security templates.** Use these .inf files to create customized security policies. You can import a predefined security template to a Group Policy object, and then customize it. For more information about security templates, see “Security Templates” in Help and Support Center for Windows Server 2003.
- **Security Configuration and Analysis.** Use this tool with a security template to analyze or configure computer security settings for the local computer. For more information about security configuration and analysis, see “Security Configuration and Analysis” in Help and Support Center for Windows Server 2003.
- **Group Policy Object Editor.** Use this tool to manage security settings in a Group Policy object for a site, domain, or OU. The Group Policy Object Editor is not part of Security Configuration Manager. However, the **Security Settings** node, which is found in the Group Policy Object Editor, is part of Security Configuration Manager. For more information about security settings, see “Security Settings” in Help and Support Center for Windows Server 2003.
- **Local security policy.** Use this tool to manage security settings on the local computer, particularly for clients who are running Windows 2000 or Windows XP Professional on Microsoft® Windows NT® or non-Microsoft networks. For more information about local security policy, see “Local security policy” in Help and Support Center for Windows Server 2003.
- **Secedit.exe.** Use this command-line tool to automate security configuration tasks. For more information about Secedit, see “Secedit” in Help and Support Center for Windows Server 2003.

Designing Security Policy

You can use GPMC to centralize the process of deploying and managing Group Policy–based security for servers running Windows 2000 Server and Windows Server 2003 and clients running Windows 2000 Professional and Windows XP Professional. Use Group Policy–based security policies to deploy and manage the following security areas:

- **Security settings.** These settings are used to define values for various security-relevant operating system parameters, such as password policy, user rights assignment, audit policy, registry values, file and registry ACLs, and service startup modes.
- **IPSec policies.** These policies are used to configure IPSec services for authenticating or encrypting network traffic. An IPSec policy consists of a set of security rules, and each security rule consists of an IP filter with an action.
- **Software restriction policies.** These policies are used to help protect computers from code that is not trusted by identifying and specifying which applications are permitted to run.
- **Wireless network policies.** These policies are used to configure settings for the Wireless Configuration Service, a user-mode service that operates on each of the IEEE 802.11 wireless network adapters that are installed on a computer.

Figure 4.2 Designing Security Policy



Important

As with all Group Policy settings, you must fully test your implementation before you deploy your security settings to your production environment. For more information about Group Policy staging and testing, see “Staging Group Policy Deployments” in this book and “Designing a Test Environment” in *Planning, Testing, and Piloting Deployment Projects* of this kit.

Designing IPSec Policies

You can use IPSec policies to filter, authenticate, or encrypt network traffic. An IPSec policy consists of a set of security rules. Each security rule consists of an IP filter with a filter action to permit or block traffic or to negotiate security. If you define a filter action to negotiate security and encrypt a specific type of traffic, you must configure additional settings, such as an authentication method for establishing trust between IPSec peers. IPSec can be configured in many different ways; therefore, you must understand IPSec in detail and test your policy configurations in lab environments before you attempt to use policies in a production environment.

For example, an IPSec policy that secures end-to-end traffic cannot be assigned to a single computer; however, an IPSec policy that only uses permit or block filtering *can* be assigned to a single computer. You must fully understand IPSec before you assign an IPSec policy. If an IPSec policy is not correctly configured and assigned, it might inadvertently block all communication to a computer.



Important

The IPSec filter lists, actions, and default policies included with Windows Server 2003 are not appropriate to use under any circumstances. They are intended *only* as examples to demonstrate behavior. Administrators must design and build their own policies, and customize the policies for their particular situation and security requirements.

For more information about IPSec policy, see “Deploying IPSec” in *Deploying Network Services* of this kit, and the *Networking Guide* of the *Windows Server 2003 Resource Kit* (or see the Networking Guide on the Web at <http://www.microsoft.com/reskit>). For more information about how to use IPSec and Group Policy, see “Assign or unassign IPSec policy in Group Policy” and “Creating, modifying, and assigning IPSec policies” in Help and Support Center for Windows Server 2003.

Assigning an IPSec policy to a GPO records a pointer to the IPSec policy that is inside the GPO attribute `ipsecOwnersReference`. The GPO itself contains only a Lightweight Directory Access Protocol (LDAP) distinguished name (DN) reference to the IPSec policy. Group Policy is used only to deliver the policy assignment to the computer’s IPSec service. The computer’s IPSec service then retrieves the IPSec policy from Active Directory, maintains a current cache of the policy locally, and keeps it current by using a polling interval that is specified in the IPSec policy itself. Because the IPSec policy itself is not stored inside the GPO, its settings can be assigned to and shared by many GPOs. Consider the following characteristics when you plan for the behavior and management of Group Policy for IPSec.

Plan IPSec Policy to Fit Your Active Directory Structure

By default, in Windows Server 2003, Active Directory restricts Read permissions on the IP Security Policies container to a greater degree than in Windows 2000. If you are deploying a new installation of Windows Server 2003 Active Directory, be aware that IPSec policies cannot be read by computers in child domains, even though the GPO can be read by computers in the child domain. The domain administrator must explicitly allow permissions for computers in child domains to read the IPSec policy from the parent domain.

For clean Windows Server 2003 installations of Active Directory, the Group Policy Creator Owners administrative group does *not* have permission by default to create or modify IPSec policies. By default, only members of the Domain Admins group have this permission, and the Group Policy Creator Owners group has read-only permission. Upgrades of Windows 2000 Active Directory domains to Windows Server 2003 domains do not change permissions on existing IPSec policy objects.

IPSec policies are stored in the IP Security Policies container. This container is separate from the GPOs to which IPSec policies are applied; therefore, the domain administrator must grant permissions to that container for others to administer IPSec policies. IPSec permissions cannot be delegated by using standard delegation tools, but instead require the use of the Active Directory Service Interfaces (ADSI) Edit tool. IPSec administrators must have Full Control or Modify permissions to all IPSec policies in that container. After the IPSec administrator creates a policy, a member of the Group Policy Creator Owners group or some other delegated owner of the GPO can assign the IPSec policy to the appropriate GPOs. For more information, see article 329194, “Permissions on the IPSec Policy Store” in the Microsoft Knowledge Base. To find this article, see the Microsoft Knowledge Base link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Unlike most Group Policy settings, multiple IPSec policies that are assigned in different GPOs are not merged. The last GPO in the Active Directory directory tree (closest to the computer object) that contains an IPSec policy assignment is the one that takes effect. Because the actual IPSec policy that is applied on the computer depends on the network adapter configuration of that computer, using the IP Security Monitor snap-in or Netsh IPSec context (the **netsh ipsec static show** and **netsh ipsec dynamic show** commands) is the only way to view the detailed IPSec policy settings as they are applied on the computer.



Note

Netsh is a command-line tool for configuring networking components on the local computer or on remote computers running Windows 2000, Windows XP Professional, or Windows Server 2003. The Netsh IPSec context is only available on Windows Server 2003. For more information about using the Netsh IPSec context, see “Netsh commands for Internet Protocol security (IPSec)” in Help and Support Center for Windows Server 2003.

Group Policy inheritance in Active Directory cannot be blocked for a specific GPO without affecting other settings in the GPO. If you must control IPSec policy inheritance, create a new GPO that is dedicated exclusively to deploying and assigning IPSec policy.

For recommendations on the uses of IPSec, see “Special IPSec considerations” in Help and Support Center for Windows Server 2003.

Ensure That Your New IPSec Policies Are Applied

When you deploy an IPSec policy by using Group Policy, Group Policy (Winlogon) polling detects changes in policy assignments within the GPOs. Additionally, during the Group Policy poll, IPSec checks whether its policy has changed regardless of whether the GPO has changed. By using the **gpupdate /target:computer** command, it detects that an IPSec policy is newly assigned in a GPO and causes the IPSec service to apply that policy. Additionally, it causes IPSec to detect if the IPSec policy has changed even though the GPO may not have changed. If an assigned IPSec policy has not changed, then no IPSec policy changes are applied to the computer. Using the **gpupdate /target:computer /force** command causes the IPSec policy agent to reload the assigned IPSec policy regardless of whether the GPO or the IPSec policy has changed.

IPSec also uses its own polling mechanism to detect a change in an IPSec policy that is already assigned (for example, a filter list change). This polling mechanism provides compatibility with previous versions of Windows, but it is no longer necessary because IPSec detects changes to IPSec policies during the Group Policy interval. However, it might be necessary to configure the IPSec polling interval to be shorter than the Group Policy polling interval during IPSec policy change rollout. Configuring the IPSec polling interval permits you to remove any changes that might have been made if problems occur or if you are using an IPSec domain policy to respond to security incidents. For more information, see article 813878, “How to Block Specific Network Protocols and Ports by Using IPSec,” in the Microsoft Knowledge Base. To find this article, see the Microsoft Knowledge Base link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

To completely delete and reload all existing IPSec policy configurations that affect communication, you must stop and then restart the IPSec service by using the **net stop policyagent** and **net start policyagent** commands. If your remote access service is configured to use Layer Two Tunneling Protocol (L2TP)/IPSec, you must restart the Routing and Remote Access service after the newly restarted IPSec service is running. Also, if an L2TP/IPSec virtual private network (VPN) client connection is connected when the IPSec service is restarted, the VPN connection is interrupted and must be reconnected.

IPSec policies cannot be applied by using security templates, and they cannot be analyzed by the Security Configuration Manager.

IPSec Differences When Using the Group Policy Management Console (GPMC)

Because the IPSec policy itself is not stored inside the GPO, note the following differences when using GPMC to manage GPOs that have IPSec policies applied:

- You can use the GPMC **Backup** and **Restore** capabilities to store information about which IPSec policies are assigned to specific Group Policy objects. However, because the IPSec policies themselves aren't stored in GPOs, you must use the **Export Policies** and **Import Policies** commands of IP Security Policy Management snap-in to back up and restore the IPSec policies themselves.
- GPMC **Delegation of rights** and **Security Filtering** permissions only apply to the GPO, not to the IPSec policy that is assigned in the GPO. Thus delegation of edit rights within GPMC only allows a user to assign or unassign an existing IPSec policy in the specific GPO, but only if the user also has read access rights to the IPSec policy. Delegation of rights to create, edit, or delete IPSec policies must be done on the IPSec policies container.
- GPMC **Import Settings** can only import an IPSec policy assignment and cannot be used to import IPSec policies into a GPO. The IP Security Policy Management snap-in provides export and import capabilities for the IPSec policy store. When using GPMC to import or copy a GPO into another domain or forest, the IPSec policy assignment is invalidated for the new GPO. The administrator must assign an IPSec policy in that domain or forest to the GPO.
- The GPMC Group Policy Results wizard is used to show which GPOs are applied to a computer, which includes the IPSec policy assignments. To find out which IPSec policy is assigned to a specific computer, after running the wizard, right-click on the computer node, and then select **Advanced View**.

Additionally, on computers running Windows XP, IPSec does not provide Resultant Set of Policy (RSOP) information. GPMC Group Policy Results shows the GPO being processed, but does not show which IPSec policy is assigned. Use **netdiag /test:ipsec** to view the assigned IPSec policy.



Note

Additional IPSec design and deployment information is not included in this chapter. For more information about deploying IPSec, see "Deploying IPSec" in *Deploying Network Services* of this kit. For more information about how to create IPSec policies, see "Creating, modifying, and assigning IPSec policies" in Help and Support Center for Windows Server 2003.

Designing Security Settings

This section discusses the recommendations and considerations for using security templates and implementing security settings. Before implementation make sure to consider the following design elements. For more information about importing security templates for domain controllers, servers, or workstations, see “Importing Security Templates and Modifying Security Settings in a GPO” later in this chapter.

Use the NTFS file system

You cannot secure Windows-based computers that are installed on file allocation table (FAT) file systems. All the security design and deployment recommendations in this chapter assume that you use the NTFS file system on all computers that you need to secure.

Complete all policy settings before applying them

Make sure that all the settings of your policy are in place before you apply the policy to any GPOs. If you apply the policy in parts, and a user refreshes the policy before all the parts are in effect, this can adversely affect the user’s computer when configuring software restriction policies.

Avoid editing the Default Domain GPO and the Default Domain Controllers GPO

The Default Domain GPO and Default Domain Controllers GPO are vital to the health of any domain. The Default Domain GPO provides the basic domain encryption key, and if that policy is removed or deleted, users cannot unencrypt their files. There are two exceptions:

- Editing the Default Domain GPO to define account policies, including password policies, account lockout policies, and Kerberos policies.
- Editing the Default Domain Controllers GPO to define user rights assignment and audit policy for the domain controllers OU.

Set domain account policy in the Default Domain GPO

When you set account policies (including password policies, account lockout policies, and Kerberos policies) in Active Directory, there can only be *one* domain account policy throughout all servers, workstations, and domain controllers in the domain. The policy is the account policy that is applied at the root domain of a domain tree. Although account policies affect user accounts, the policies are defined on computers.

Do not link to a GPO in another domain

Avoid linking to a GPO in another domain because this can degrade performance.

Consider precedence of policy application when multiple GPOs are applied

Because a computer can have more than one GPO applied to it, security settings can conflict. From highest to lowest, the settings apply in the following order of precedence: OU, domain, site, and local computer. For example, policies that are defined in Active Directory at the OU, domain, or site level always override the local security policy for a computer if there is a conflict. If the same computer is a member of an OU, the organizational unit policy overrides all other settings. If the computer is a member of nested OUs, the OU that immediately contains the computer takes precedence.

For nested OUs, the GPO that is linked closest to the OU takes precedence. The precedence rules that apply to restricted groups also apply to other Group Policy settings when there is a conflict. For example, if a computer is a member of OU A, which is nested in OU B, and both OUs define Power Users as a restricted group, then the definition of Power Users according to OU A takes precedence on the computer.

To find out which policies are currently applied to a specific computer, use the **Group Policy Results** node in the GPMC snap-in.

Plan Event log size and wrapping according to business and security requirements

Define Event log size and overwrite of events logs (also known as *log wrapping*) to match the business and security requirements of your organization's security plan. Implement these Event log settings at the site, domain, or OU level to take advantage of Group Policy settings.

Understand the use of Restricted Groups

If you create a Restricted Groups policy for a group, any users and groups that are not specified as members of the group within the policy are removed from the group. For example, if you create a Restricted Groups policy for the local Administrators group, and the newly created policy specifies only the Domain Admins group as members, all other members of the local Administrators group (including any local accounts) are removed from the local Administrators group when the policy is applied. Note that if the Restricted Groups members are defined in more than one GPO, only the members that are defined in the GPO with the highest precedence are applied. This also applies to the groups that the group can be a member of.

Be aware that security settings can persist

For Windows Server 2003 and Windows XP, security settings might persist even if the setting is no longer defined in the GPO that originally applied it. This occurs under the following conditions:

- The setting was not defined for the local computer at the time that the policy setting was applied.
- The setting is for a registry object.
- The setting is for a file system object.

Windows 2000 security settings may persist even if the setting is no longer defined in the GPO that originally applied it. This occurs under the following conditions:

- The setting has not been defined for the local computer at the time that the policy setting was applied.
- The setting is for a registry object.
- The setting is for a file system object.
- The setting is for a service.
- The setting is for a Restricted Groups policy.
- The setting is an Event log setting.

All settings that are applied through local policy or a GPO are stored in a local database on your computer. Whenever a security setting is modified, the computer saves the security setting value to the local database. The database retains a history of all the settings that have been applied to the computer. If a policy defines a security setting and then no longer defines that setting, the setting reverts to the previous value in the database. If a previous value does not exist in the database, the setting remains defined as is. This behavior is sometimes called *tattooing*.

Any other settings that persist maintain the values that are applied through the policy until that setting is set to a different value.

Using Custom Security Templates

Security templates are files that represent a security configuration. These files can be imported to a GPO, applied to a local computer, or used to analyze security. To edit individual security settings on a domain, site, or OU, administrators use the Group Policy Object Editor.

You can view the templates as text files or you can use the Security Templates snap-in to view the settings in each template. Security templates can be transported, imported, and exported. All of the security attributes in Table 4.1 can be contained in a security template.

Table 4.1 Security Template Attributes

Security Attribute	Description
Account Policies	Password policy, account lockout policy, and Kerberos policy
Local Policies	Audit policy, user rights assignment, and other security options, including numerous security-related registry values
Event Log	Application, system, and security Event log settings
Restricted Groups	Membership of security-sensitive groups
System Services	Startup and permissions for system services
Registry	Permissions and auditing entries for registry keys
File System	Permissions and auditing entries for folders and files

Selecting Predefined Security Templates

Windows Server 2003 includes a set of predefined security templates that you can use to create customized security policies. You can customize the templates by using the Security Templates snap-in. It is recommended that you save one of the predefined templates under another name, and then modify it to meet the needs of your organization. You can use a template to configure either a single computer or an entire domain. You can also use a security template — with the Security Configuration and Analysis snap-in — as a baseline for analyzing the local computer for potential security problems or policy violations.

The default storage location of the predefined security templates is %systemroot%\Security\Templates. Only administrators have permissions to modify the templates in this folder; users without administrative permissions can save their templates to another folder. This folder includes the following templates.

Setup Security.inf

Setup security.inf is a computer-specific template that represents the default security settings that are applied when the operating system is installed, including the file permissions for the root of the system drive.

The Setup security.inf template is created for each computer during installation. It can vary from computer to computer and is based on whether the installation was a clean installation or an upgrade. This template can be used on servers and client computers; it cannot be applied to domain controllers. You can apply portions of this template for disaster recovery purposes.

Do not apply Setup security.inf using Group Policy. It contains a large amount of data and can seriously degrade performance if it is applied by using Group Policy. Degraded performance can occur because policy is periodically refreshed, and a large amount of data then moves through the domain.

It is recommended that you apply the Setup security.inf template in parts by using the Secedit command-line tool. For more information about Secedit, see “Secedit” in Help and Support Center for Windows Server 2003.

DC Security.inf

This template is created when Active Directory is installed onto a server. It reflects file, registry, and system service default security settings. Reapplying this template resets these settings to default values. Note that this template might overwrite permissions on new files, registry keys, and system services that are created by other applications. It can be applied by using the Security Configuration and Analysis snap-in or the Secedit command-line tool.

Compatws.inf

Default permissions for workstations and servers are primarily granted to three local groups: Administrators, Power Users, and Users. Of the three, the Administrators group has the most permissions, while the Users group has the least. Because of this, you can significantly improve security, reliability, and the total cost of system ownership by:

- Making sure that end users are members of the Users group.
- Deploying applications that can be run successfully by members of the Users group.

Members of the Users group can successfully run applications that are a part of the Windows Logo Program. However, members of the Users group might not be able to run applications that do not meet the requirements of the program. If other applications must be supported, there are two options:

- Permit members of the Users group to be members of the Power Users group.
- Relax the default permissions that are granted to the Users group.

Because Power Users have additional permissions such as creating users, groups, printers, and shares, some administrators prefer to relax the default User permissions instead of permitting members of the Users group to be members of the Power Users group. This is precisely what the Compatible template is for. The Compatible template changes the default file and registry permissions that are granted to the Users group in a way that is consistent with the requirements of most applications that do not belong to the Windows Logo Program. Additionally, because it is assumed that the administrator who is applying the Compatible template does not want members of the Users group to be Power Users, the Compatible template also removes all members of the Power Users group. For more information, see “Default security settings for groups” in Help and Support Center for Windows Server 2003.

For more information about the Windows Logo Program for Software, see the Windows Logo Program for Software link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Do not apply the Compatible template to domain controllers. For example, do not import the Compatible template to the Default Domain GPO or the Default Domain Controllers GPO.

Secure*.inf

The Secure templates define enhanced security settings that are least likely to impact application compatibility. For example, the Secure templates define stronger password, lockout, and audit settings.

The Secure templates prevent anonymous users, such as users from untrusted domains, from:

- Enumerating account names and shares.
- Performing SID-to-name or name-to-SID translations. If this is allowed, anonymous users can request user names (such as the administrator’s user name) based on the user’s security ID (SID) as well as requesting the SID for a user based on the user name.

The Secure templates enable server-side server message block (SMB) packet signing. By default, SMB packet signing is disabled for member servers. Because client-side SMB packet signing is enabled by default, SMB packet signing is always negotiated when workstations and servers are operating at the Secure level.

Additionally, the Secure templates limit the use of LAN Manager and NTLM authentication protocols by configuring clients to send only NTLM version 2 (NTLMv2) responses and by configuring servers to refuse LAN Manager responses.

Considerations for applying Securews.inf to a member computer include:

- All domain controllers that contain the accounts of all users that log on to the client must run Windows NT 4.0 Service Pack 4 (SP4) or later, Windows 2000, or Windows Server 2003.
- If the member computer is joined to a domain that contains domain controllers that are running Windows NT 4.0, the clocks on both the domain controllers and the member computers must be set within 30 minutes of each other.

If a client is configured with `Securews.inf`, it cannot connect to:

- Servers that only use the LAN Manager authentication protocol or that run Windows NT 4.0 Service Pack 3 (SP3) or earlier using a local account that is defined on the target server.
- Servers running Windows 2000 SP3 and earlier or Windows NT 4.0 using a local account that is defined on the target server unless the clock on the target server is set within 30 minutes of the clock on the client.
- Computers running Windows XP by using a local account that is defined on the target computer unless the clock on the target computer is set within 36 hours of the clock on the client.
- Servers running LAN Manager that are running in share-level security mode.

If a server is configured with `Securews.inf`:

- A user with a local account on the server cannot connect to the server by using that local account from a client computer that is running only LAN Manager.
- For Windows 2000 SP3 and earlier, a client using a local account on the server that is also configured to use NTLMv2 authentication cannot connect unless the clocks on the two computers are set within 30 minutes of each other.

Likewise, if a domain controller is configured with `Securedc.inf`, a user who has an account in that domain cannot connect to any member server from a client computer that is running only LAN Manager using that domain account.

You can configure computers running Windows NT SP4, Windows 2000, Windows XP, or Windows Server 2003 to send only NTLMv2 responses by doing at least one of the following:

- Specify this preference in the **Network security: LAN Manager Authentication Level security** option.
- Set `HKLM\System\CurrentControlSet\Control\LSA\LMCompatibilityLevel` to 3 or higher.



Caution

Do not edit the registry unless you have no alternative. The registry editor bypasses standard safeguards, allowing settings that can damage your system, or even require you to reinstall Windows. If you must edit the registry, back it up first and see the Registry Reference on the *Windows Server 2003 Deployment Kit* companion CD or at <http://www.microsoft.com/reskit>.

Computers that run LAN Manager include Windows for Workgroups and Microsoft® Windows® 95 and Microsoft® Windows® 98 platforms that do not have the Active Directory Client Extensions Pack installed. If the Active Directory Client Extensions Pack is installed on Windows 95 or Windows 98, those clients can use NTLMv2. Microsoft® Windows® Millennium Edition supports NTLMv2 without additional modification.

Hisec*.inf

The Highly Secure templates are supersets of the Secure templates that require greater levels of encryption and signing for authentication and for the data that flows over secure channels and between SMB clients and servers. For example, the Secure templates cause servers to refuse LAN Manager responses; the Highly Secure templates cause servers to refuse both LAN Manager and NTLM responses. The Secure template enables server-side SMB packet signing; the Highly Secure template requires it.

The Highly Secure templates limit the use of cached logon data, such as data stored by Winlogon and Stored User Names and Passwords.

Hisecws.inf uses Restricted Group settings to:

- Remove all members of the Power Users group.
- Make sure that only the Domain Admins group and the local Administrator account are members of the local Administrators group.

Hisecws.inf defines these group restrictions under the assumption that users only use applications that belong to the Windows Logo Program. When using those applications, neither the Compatible template nor the Power Users group is needed. Instead, users can run those applications successfully under the secure context of a member of the Users group. The Users group is defined by the default security settings of the file system and registry. Members of the Administrators group can still use any application.

Additionally, the Highly Secure templates require strong encryption and signing for the secure channel data that constitutes domain-to-member and domain-to-domain trust relationships. Thus, consideration for applying Hisecws.inf to a member computer include:

- All of the domain controllers that contain the accounts of all users that can log on to the client must be running Windows NT 4.0 SP4 or later, Windows 2000, or Windows Server 2003.
- All of the domain controllers for the domain that the client is joined to must run Windows 2000 or Windows Server 2003.

Clients that are configured with Hisecws.inf cannot connect to:

- Computers that only run LAN Manager or computers running Windows NT 4.0 SP3 or earlier using a local account defined on the target server.
- Servers running Windows 2000 SP3 and earlier or Windows NT 4.0 SP4 using a local account that is defined on the target server unless the clock on the target server is set within 30 minutes of the clock on the client.
- Computers running Windows XP using a local account that is defined on the target computer unless the clock on the target computer is set within 36 hours of the clock on the client.
- LAN Manager servers that are operating in share-level security mode.

To apply Hisecdc.inf to a domain controller, all of the domain controllers in all trusted or trusting domains must run Windows 2000 or Windows Server 2003 operating systems.

If a server is configured with Hisecws.inf:

- A user who has a local account on that server cannot connect to that server from a client that does not support NTLMv2.
- A client that has a local account on that server cannot connect to that server unless the client is configured to send NTLMv2 responses.
- All clients that want to use SMB to connect to the server must enable client-side SMB packet signing. By default, all clients running Windows 2000 and Windows XP operating systems enable client-side SMB packet signing.

If a domain controller is configured with Hisecdc.inf:

- If a user attempts to connect to member servers by using a domain account in the same domain, the connection will fail if the user's client only uses the LAN Manager authentication protocol.
- LDAP clients cannot bind with the Active Directory LDAP server unless data signing is negotiated. LDAP BIND requests using `ldap_simple_bind` or `ldap_simple_bind_s` are rejected. By default, all Microsoft LDAP clients included with Windows XP request data signing if Transport Layer Security/Secure Sockets Layer (TLS/SSL) is not already being used. If TLS/SSL is being used, data signing is negotiated.
- A user who has an account in that domain cannot connect to member servers by using that domain account unless:
 - Both the client and target server are running Windows 2000, Windows XP, or Windows Server 2003, and both can use Kerberos-based authentication instead of LAN Manager-based authentication.
 - The client is configured to send NTLMv2 responses.

Rootsec.inf

Rootsec.inf specifies the root permissions. By default, Rootsec.inf defines these permissions for the root of the system drive. This template can be used to reapply the root directory permissions if they are inadvertently changed, or the template can be modified to apply the same root permissions to other volumes. As specified, the template does not overwrite explicit permissions that are defined on child objects; it propagates only the permissions that are inherited by child objects.

Notssid.inf

The default file system and registry ACLs on servers assign permissions to a Terminal Server security identifier (SID). The Terminal Server SID is used only when Terminal Server is running in application compatibility mode. If Terminal Server is not being used, this template can be applied to remove the Terminal Server SIDs that are not necessary from the file system and registry locations. However, removing the access control entry (ACE) for the Terminal Server SID from these default file system and registry locations does not increase the security of the system. Instead of removing the Terminal Server SID, run Terminal Server in Full Security mode. When you run Terminal Server in Full Security mode, the Terminal Server SID is not used.

Design Recommendations for Using Predefined Security Templates

The Windows Server 2003 security templates are for computers that use the default security settings. These templates incrementally modify the default security settings if they are on the computer. They do not install the default security settings before performing the modifications.

Consider the following recommendations before you use the predefined security templates.

Read the security template descriptions before you select which template to use

To successfully deploy the security templates, you need to understand which template is appropriate for your computer.

Use the Setup security.inf template only on the local computer

Do not apply the Setup security.inf template using Group Policy. Apply it only to the local computer by using the Security Configuration and Analysis snap-in or the Secedit.exe command-line tool. The Setup security.inf template is modified during installation and is created specifically for each computer. It might vary from computer to computer. This template contains a large amount of data and can degrade performance if it is applied by using Group Policy. This occurs because Group Policy is refreshed periodically, and a large amount of data is moving through the network each time the policy is refreshed. The advantage of using the Secedit.exe command-line tool to apply Setup security.inf is that the command-line tool permits you to configure subareas of the default settings. For example, by using Secedit.exe, you can apply only the default file system ACLs without also resetting the user rights and registry ACLs.

Apply workstation, server, and domain controller templates appropriately

Apply templates of the form *ws.inf *only* to workstation or server computers; do not apply *ws.inf to domain controllers. Likewise, apply templates of the form *dc.inf *only* to domain controller class machines; do not apply *dc.inf to workstations or servers. If you apply a predefined template at the domain root level, it applies to all computers in the domain by default. For example, account policies (password policies, account lockout policies, and Kerberos policies) are always defined at the domain level, but local policies are subject to precedence rules.

Use Group Policy to apply templates to groups of computers

You can import a security template to a Group Policy object to make sure that any computers where the Group Policy object is applied automatically receive the template's security settings when the Group Policy settings are refreshed.

Use the appropriate tools to apply templates to local computers

Configure individual computers by using the Security Configuration and Analysis snap-in, the Secedit.exe command-line tool, or by importing the template into the local security policy. Configure groups of computers by importing a template into the Group Policy Object Editor.

For more information about importing security templates for domain controllers, servers, or workstations, see "Import a security template to a Group Policy object" in Help and Support Center for Windows Server 2003.

Refreshing Group Policy to Activate New Settings

If any changes are made to the settings, all Group Policy settings are refreshed automatically every 90 minutes on a workstation or server and every five minutes on a domain controller. Additionally, security settings are refreshed every 16 hours, regardless of whether any changes have been made.

Security settings are also refreshed when you restart the computer, and you can trigger a Group Policy object refresh to apply a newly deployed GPO, including security settings. You can do so by using the **gpupdate** command. The **gpupdate** command replaces the **/refreshpolicy** option that was previously used for the **secedit** command.

For more information about the **gpupdate** command including full syntax, see “Gpupdate” in Help and Support Center for Windows Server 2003.

Designing Software Restriction Policies

Software restriction policies permit you to identify software that is running on computers in your domain and to control its ability to run. By using software restriction policies, you can:

- Control which programs can run on your system. For example, you can control which types of programs can be accepted as e-mail attachments if you are concerned about users being sent e-mail viruses.
- Run only digitally signed scripts.
- Permit users to run only specific files on multiuser computers. For example, you might want to lock down specific executable files in specific directories on a terminal server.
- Decide who can add trusted publishers to a computer.
- Control whether software restriction policies affect all users or only specific users who use a computer.
- Prevent any files from running on a local computer.

Consider the following design recommendations before you create rules and apply software restriction policies:

- Decide if you want the policy to apply to multiple computers or users in a domain or OU or if you want it only to apply to the local computer. If you want the policy to apply to many computers or users in a domain or other Active Directory container, use a GPO. If you want the policy to apply only to the local computer, use the Local Security Policy snap-in.
- Decide if you want the policy to apply to users or computers. Applying a policy to users affects the users regardless of which computer they use to log on to the network. Applying a policy to computers affects the computers regardless of which users log on.

- Decide what the default security level of the policies will be. The default security level can either be **Disallowed**, which does not permit software to run, or **Unrestricted**, which permits software to run with the full permissions of the user who is logged on. After you have decided what the default security level will be, you can begin creating rules. The Rules types are:
 - **Hash rules.** Software is identified by its hash.
 - **Certificate rules.** Software is identified by its signing certificate.
 - **Path rules.** Software is identified by its file path or registry path.
 - **Internet zone rules.** Software is identified by using a zone that is specified by Microsoft® Internet Explorer. Zone rules apply only to Windows Installer packages.

For more information about deploying software restriction policies, see:

- “Deploying a Managed Software Environment” in this book.
- The Software Restriction Policies link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.
- “Software restriction policies” in Help and Support Center for Windows Server 2003.

Designing Wireless Network Policies

Administrators can define policy settings to help secure wireless network configurations for both the IEEE 802.11 configuration and the IEEE 802.1X authentication engine. If you use Group Policy for wireless networking, the policy settings that are defined in the GPO that affects a specific computer take precedence over the user-defined settings. The type of network that you use also affects precedence. You can design wireless network policies for three types of networks:

- **Access point (infrastructure).** In this type of network, wireless devices with radio network adapters, such as a portable computer or personal digital assistant, connect to wireless access points.
- **Computer-to-computer (ad hoc).** In this type of network, wireless devices connect to each other directly instead of through wireless access points.
- **Any available network access point preferred.** When you select this option, a connection to an access point wireless network is always attempted first, if one is available. If an access point network is not available, a connection to a computer-to-computer wireless network is attempted.

The wireless networking technologies that are included in Windows XP Professional and Windows Server 2003 support the IEEE 802.11 and IEEE 802.1X standards for wireless communications. For complete information about deploying these technologies, see “Deploying a Wireless LAN” in *Deploying Network Services* of this kit. For step-by-step information about creating wireless network policies, see “Wireless networking” in Help and Support Center for Windows Server 2003.

Design Considerations for Wireless Network Policies

Consider the following issues that pertain to authentication methods and wireless network policies:

- Computer authentication is recommended. By default, authentication is set to **Enabled**.
- The access point must support the authentication method that you select. For example, the access point must support 802.1X. If you choose EAP-TLS, all computers must support it (for example, a RADIUS server must support EAP-TLS).
- Your servers and wireless clients must support the authentication method you plan to deploy. Whether you choose EAP-TLS or PEAP as the authentication method over 802.1X, both your RADIUS server and your wireless clients need to support it.
- It is recommended that you permit certificate autoenrollment for users and computer when you use EAP-TLS. For more information, see “Checklist: Configuring certificate autoenrollment” in Help and Support Center for Windows Server 2003.
- The wireless network configuration settings that are defined in GPOs take precedence over user-defined settings. The only exception to this is the list of preferred networks, where the policy-defined list is merged with the user-defined list. For more information, see “Implementing Wireless Network Policies” later in this chapter.
- If a domain policy for wireless configuration exists, the local user (whether the user is an administrator or non-administrator) cannot remove or disable the domain policy.
- When a Group Policy change occurs, the Wireless Configuration service breaks the current association *if and only if* the new policy takes precedence (for example, a visible network is now a more preferred network according to the policy’s list of preferred networks). In all other cases, the association does not change.
- If a GPO that contains wireless network policies is deleted, the Wireless Configuration service clears its policy cache, initiates and processes a soft reset, and then reverts to the user-configured settings.

Understanding Wireless Network Policy Precedence

If wireless network configuration settings have been defined both on the local computer (by the user) and in a GPO that affects that computer, the wireless network settings are merged, and the user cannot change the Group Policy wireless network settings. One exception to this rule is the Wired Equivalent Privacy (WEP) key. The user also cannot change the order in which the settings are applied. The wireless networks can be access point (infrastructure) or computer-to-computer (ad hoc) networks. The merging process and order of precedence occur according to the following rules:

- Infrastructure networks *always* have higher precedence than ad hoc networks.
- Group Policy overrides user-defined policy, and the wireless network policy configurations have the highest precedence of their respective group of configurations (infrastructure or ad hoc).

For example, an administrator might define a GPO with the following wireless configuration settings, and then select **The key is provided for me automatically** option:

- Service Set Identifier (SSID): any
- Network type: either infrastructure or ad hoc
- Authentication mode: either open or shared
- Encryption: WEP

In this case, the user can clear the **The key is provided for me automatically** check box, and type in different key information because WEP key configuration can be changed locally.

Example: Preferred Network Precedence

This example illustrates how the merging and ordering process occurs. The client computer is a member of WirelessClientsOU. A GPO named WirelessConfigGPO is assigned to WirelessClientsOU, and the GPO defines the following list of preferred networks:

- Infrastructure network Ip1
- Infrastructure network Ip2
- Ad hoc network Ap1
- Ad hoc network Ap2

The client computer has this list of user-defined preferred networks (local):

- Infrastructure network Iu1, which is user defined and the same network as Ip1.
- Infrastructure network Iu2, which is user defined and the same network as Ip2.
- Infrastructure network Iu3.
- Ad hoc network Au2, which is the same network as Ap2.
- Ad hoc network Au3.

When the GPO is applied to that client, the resulting list of preferred networks is merged in the following order: Ip1, Ip2, Iu3, Ap1, Ap2, and Au3. This occurs because infrastructure networks take precedence over ad hoc networks and because settings in the OU take precedence over local settings. For example, Ip1 and Iu1 are the same network with different configurations; Ip1 is configured by a Group Policy, and Iu1 is configured locally.

For more information, see “Define wireless network policies on a client computer” and “Define Active Directory–based wireless network policies” in Help and Support Center for Windows Server 2003.

Multiple GPOs

If a computer is subject to multiple GPOs that contain wireless network policies, the wireless settings that are defined in the GPO associated with the Active Directory container closest to the computer object takes precedence. Those settings will override the settings that are assigned to a higher level Active Directory container. In this case, the settings are not merged. For example, a client is a member of OU1 in the Redmond domain, and the following GPOs are being used:

- **GPOA.** This GPO defines wireless network policies and is assigned to the Redmond domain.
- **GPO1.** This GPO contains wireless policy settings and is assigned to OU1. The client is a member of this OU.

When the GPO list for this client is processed, the GPO1 wireless network settings take precedence and are in effect for this computer. The settings are not merged.

Measuring Your Design Using the GPMC

In Windows Server 2003, you can use the Group Policy Results Wizard in the GPMC to view information about the following settings defined in your wireless network policies:

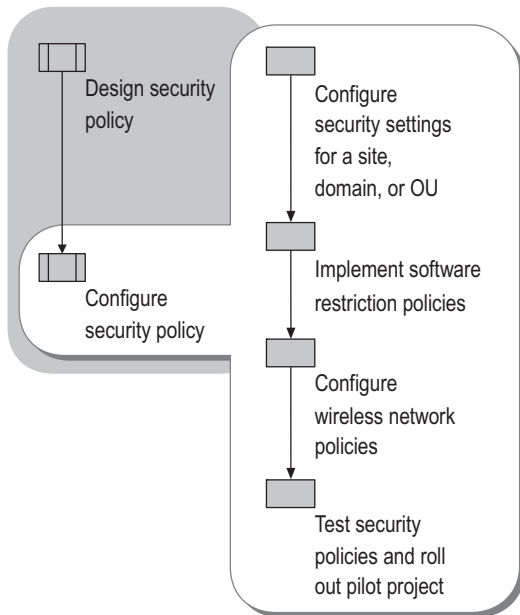
- The preferred list of wireless networks to which clients can connect
- The wireless network association settings
- The IEEE 802.1X authentication and settings

The Group Policy Results wizard replaces the Resultant Set of Policy (RSOP) – Logging Mode capabilities. For step-by-step information about using the Group Policy Results wizard, see “How to create a new Group Policy Results query” in GPMC Help.

Configuring Security Policy

You can use Group Policy to manage all of the computers in your organization from one computer. By using GPMC, you can create and edit policies that affect workstations, servers, and domain controllers throughout your organization. Figure 4.3 shows which security settings to configure.

Figure 4.3 Configuring Security Policy



Configuring Security Settings for Sites, Domains, and OUs

By using the Group Policy Object Editor, you can modify individual security settings in a GPO, or you can import a template to a GPO that is linked to an OU, domain, or site. If you want to change the default security settings on your computers, there are several ways to configure security settings on multiple computers.

Before you make any changes, make sure that you understand the default security settings. For more information, see “Default security settings for groups” and “Default groups” in Help and Support Center for Windows Server 2003. For information about the default setting for each policy, see “Security setting descriptions” in Help and Support Center for Windows Server 2003.

Importing Security Templates and Modifying Security Settings in a GPO

By using Group Policy Object Editor and a security template, you can create a security policy for your computers. You can use GPMC to navigate to any GPO in the forest, and then open the Group Policy Object Editor. The Group Policy Object Editor permits you to import security templates and edit security settings. The security template is a single location that contains the full range of security settings. After you have imported the security template, you can edit individual policies.

► To import a security template for a domain or OU

1. Open GPMC.
2. In the console tree, expand the domain or OU that you want to manage, right-click the Group Policy object that you want to edit, and then click **Edit**.
3. In the Group Policy Object Editor console tree, click **Computer Configuration**, click **Windows Settings**, right-click **Security Settings**, and then select **Import Policy**.
4. Click the security template that you want to import, and then click **Open**.

For step-by-step information about configuring security templates, see “Security Templates” in Help and Support Center for Windows Server 2003.

After you have imported a template to the GPO, you can manually modify the security settings in the GPO.

► **To modify security settings**

1. Open GPMC.
2. In the console tree, expand the domain or OU that you want to manage, right-click the Group Policy object that you want to edit, and then click **Edit**.
3. In the Group Policy Object Editor console tree, click **Computer Configuration**, click **Windows Settings**, and then click **Security Settings**.
4. Do one of the following:
 - To edit **Password Policy**, **Account Lockout Policy**, or **Kerberos Policy**, click **Account policies**. Before making any changes to these policies make sure you understand how account policies are applied. For more information, see “Modifying Account Policies in the Default Domain GPO” later in this section.
 - To edit **Audit Policy**, **User Rights Assignment**, or **Security Options**, click **Local Policies**.
 - To edit Event log settings, click **Event Log**.
5. In the details pane, double-click the security setting that you want to modify.
6. If the security settings have not been defined, you can click to select the **Define these policy settings** check box.
7. Modify the security settings, and then click **OK**.

For step-by-step information about configuring security templates, see “Security Templates” in Help and Support Center for Windows Server 2003.

Modifying Account Policies in the Default Domain GPO

Account policies include password policy, account lockout policy, and Kerberos policy. Although they affect user accounts, account policies are defined on computers. In Windows Server 2003 and Windows 2000, there is only one set of account policies for each domain, and these policies are defined at the domain level.

The account policies for the domain affect all users who log on to the domain, regardless of any other account policies that are defined in a linked GPO. However, if a user logs on to a member computer by using a local computer account, the user is subject to the usual order of precedence as described in “Designing Security Settings” earlier in this chapter. Domain controllers do not have local accounts and always receive account policies from the domain.

If you want to modify the account policies at the domain level, it is recommended that you modify the default domain GPO. The account policies for domains include:

- **Password policy settings for domains.** The most common way to authenticate a user's identity is by using passwords. After a user has been identified and authenticated, the user can perform any tasks or access any resource for which he or she is authorized. Strong passwords generally enhance security for users. Using strong passwords helps avoid the threat of an unauthorized user guessing a weak password (also known as *cracking*) and acquiring the credentials of the compromised user account (also known as *spoofing*). This is especially true for administrative accounts because an unauthorized user might obtain administrative credentials and gain elevated privileges. For more information, see "Strong passwords" in Help and Support Center for Windows Server 2003.
- **Account lockout policy settings for domains.** More than a few unsuccessful password tries during logon might represent an attacker's attempt to determine an account password by trial and error. Windows Server 2003 and Windows 2000 tracks the number of logon attempts, and it can be configured to respond to this type of attack by disabling the account for a preset period of time. This is known as an account lockout.
- **Kerberos policy settings for domains.** Kerberos V5 authentication protocol provides the default mechanism for authentication services and the authorization data that is necessary for a user to gain access and perform a task on a resource. By reducing the lifetime of Kerberos authentication tickets, you reduce the risk of having a legitimate user's credentials stolen and successfully used by an attacker. However, authorization overhead is increased.

In addition, there are five Security Option settings that behave in the same way as account policies. These are:

- Network Security: Force logoff when logon hours expire
- Accounts: Administrator account status
- Accounts: Guest account status
- Accounts: Rename administrator account
- Accounts: Rename guest account

For more information about the individual account policies, see "Account policies" in Help and Support Center for Windows Server 2003.

Modifying Local Policies in the Default Domain Controllers GPO

You can establish local policies to secure your domain controllers. Local policies are divided into a number of settings categories, including:

- **User rights assignment.** User rights permit users to log on and perform specific administrative or operations tasks on your domain controllers. Make sure that the appropriate user rights are assigned to users in the domain so that the users can perform their intended functions without compromising the security of the domain controllers.



Important

Make changes to the user rights assignment policy settings directly in the Default Domain Controllers GPO for application compatibility reasons. Not doing so can cause unexpected behavior if server applications are later installed on the domain controller.

- **Audit policy settings.** When you enable auditing on your domain controllers, the number of events that is recorded in the security event log increases. As a result, the maximum size of the security event log must be increased. As a part of your typical operations tasks, archive the security and system event logs regularly and frequently before they fill up. If the logs fill up, you might miss events.



Important

Make changes to the audit policy settings directly in the Default Domain Controllers GPO for application compatibility reasons. Not doing so can cause unexpected behavior if server applications are later installed on the domain controller.

- **Security options policy settings.** The domain controller security options policy settings affect Active Directory–related security configuration settings and network, file system, and user logon security configuration settings.

For more information about securing domain controllers, see the Securing Active Directory Installations link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Implementing Software Restriction Policies

By using software restriction policies, you can protect your computer or network by identifying and specifying the software that is permitted to run. The first step is to set the security level for a computer to **Unrestricted** or **Disallowed**. If the default level of security is set to **Unrestricted**, users can run all programs, except for the programs that you restrict by using rules. If the default security level is **Disallowed**, no programs can run on the computer, except the programs that meet the requirements of the rules. After you set a default security level to **Unrestricted** or **Disallowed**, you can make exceptions to the default security level by creating software restriction policy rules.

Rule Precedence

Rules are evaluated in a specific order. The rules that more specifically match a program take precedence over rules that more generally match a program. From highest to lowest, rule precedence is as follows:

- Hash rule
- Certificate rule
- Path rule
- Internet zone rule
- Default security level

Example of Rule Precedence with a Default Security Level of Unrestricted

Table 4.2 shows an example of rules that are configured by using software restriction policies on a computer that has a default security level of **Unrestricted**.

Table 4.2 Example of Software Restriction Policy Rules

Rule	Type of Rule	Description	Setting
Rule 1	Hash rule	Hash of Pagefileconfig.vbs	Disallowed
Rule 2	Certificate rule	IT management certificate	Unrestricted
Rule 3	Path rule	%WINDIR%\System32*.VBS	Unrestricted
Rule 4	Path rule	*.VBS	Disallowed
Rule 5	Path rule	%WINDIR%	Unrestricted

Table 4.3 shows examples of how the software restriction policy rules in Table 4.2 determine which programs users can run.

Table 4.3 Example of the Application of Software Restriction Policy Rules

Program Started	Applied Rules	Outcome
C:\WINDOWS\SYSTEM32\EventQuery.vbs	<p>Rule 3 is applied because EventQuery.vbs is a .vbs file in the System32 folder.</p> <p>Rule 4 is applied because EventQuery.vbs has a .vbs extension.</p> <p>Rule 5 is applied because EventQuery.vbs is stored in a subfolder of the Windows folder.</p>	<p>Rule 3 is the most specific match for EventQuery.vbs. Because Rule 3 has a security level of Unrestricted, EventQuery.vbs is permitted to run.</p>
C:\WINDOWS\SYSTEM32\Pagefileconfig.vbs	<p>Rule 1 is applied because the hash in the rule matches the hash of Pagefileconfig.vbs.</p> <p>Rule 3 is applied because Pagefileconfig.vbs is a .vbs file in the System32 folder.</p> <p>Rule 4 is applied because Pagefileconfig.vbs has a .vbs extension.</p> <p>Rule 5 is applied because Pagefileconfig.vbs is stored in a subfolder of the Windows folder.</p>	<p>Rule 1 is the most specific match for Pagefileconfig.vbs. Because Rule 1 has a security level of Disallowed, Pagefileconfig.vbs is not permitted to run.</p>
\\LOGIN_SRV\Scripts\CustomerScript1.vbs	<p>Rule 2 is applied because CustomerScript1.vbs is digitally signed by the certificate that belongs to the customer's IT management group.</p> <p>Rule 4 is applied because CustomerScript1.vbs has a .vbs extension.</p>	<p>Rule 2 is the most specific match for CustomerScript1.vbs. Because Rule 2 has a security level of Unrestricted, CustomerScript1.vbs is permitted to run.</p>
C:\Documents and Settings\user1\LOVE-LETTER-FOR-YOU.TXT.VBS	<p>Rule 4 is applied because LOVE-LETTER-FOR-YOU.TXT.VBS has a .vbs extension.</p>	<p>Rule 4 is the most specific match for LOVE-LETTER-FOR-YOU.TXT.VBS. Because the Rule 4 has a security level of Disallowed, LOVE-LETTER-FOR-YOU.TXT.VBS is not permitted.</p>

DLL Checking

Most programs require multiple .dll files to run. By default, software restriction policy rules are not enforced against .dll files. This is the recommended option for most users for the following reasons:

- Setting a program's main executable file as **Disallowed** in the Software Restriction Policies snap-in prevents the program from running. Therefore, it is typically not necessary to set all of the related .dll files to **Disallowed**.
- Checking .dll files results in performance degradation on the system. If a user runs 10 programs during his or her logon session, the software restriction policy is evaluated 10 times. If .dll checking is turned on, the software restriction policy is evaluated for each .dll file that is loaded with each program. For example, if each program uses 20 .dll files, 10 .exe files are checked, and then 200 .dll files are checked. The software restriction policy is evaluated 210 times.
- If the default security level is set to **Disallowed**, the main executable file has to be identified so that it can run, and all of the executable file's .dll files must be identified.

To activate .dll checking, in the **Enforcement Properties** policy, set **Apply software restriction policies to the following** to **All software files**. For more information about .dll checking, see "Apply software restriction policies to DLLs" in Help and Support Center for Windows Server 2003.

Exclude Administrators

You might want to prevent most users from running certain programs by setting them as **Disallowed** but permit administrators to run any programs. For example, a user might have a shared computer that multiple users connect to by using Terminal Server. You might want the users to run specific applications on the computer, while permitting members of the Local Administrators group to run any programs. To exclude local administrators, you can set the option to apply software restriction policies to **All users except local administrators**.



Note

Setting the software restriction policies to exclude local administrators is only valid for Group Policy objects that are applied to computers.

For more information about software restriction policies, see "Prevent software restriction policies from applying to local administrators" and "Software restriction policies" in Help and Support Center for Windows Server 2003, and "Deploying a Managed Software Environment" in this book.

Configuring Wireless Network Policies

Wireless network settings can be configured locally, by users on client computers, or centrally. To enhance the deployment and administration of wireless networks, you can use Group Policy to centrally create, modify, and assign wireless network policies for Active Directory clients. When you use Group Policy to define wireless network policies, you can configure wireless network connection settings, enable IEEE 802.1X authentication for wireless network connections, and specify the preferred wireless networks that clients can connect to. When you create and configure wireless policies, you have the options that are described in Table 4.4. For more information about configuring wireless policies, see “Define Active Directory-based wireless network policies” in Help and Support Center for Windows Server 2003.

Table 4.4 Configuration Settings for General Policy

Options	Comments
Name	Name of the policy. Use a unique and descriptive name of up to 255 characters that easily identifies the policy.
Check for policy changes every	Specifies in minutes how often to poll Active Directory for changes to this policy. Applies only to computers that are members of an Active Directory domain. The default is 180 minutes.
Network to access <ul style="list-style-type: none"> Any available network (access point preferred) Access point (infrastructure) networks only Computer-to-computer (ad hoc) networks only 	Specifies the types of IEEE 802.11 wireless networks that are available for clients to try to connect to.
Use Windows to configure my wireless network settings	Specifies whether client settings are automatically configured for IEEE 802.11 wireless network connections.
Automatically connect to non-preferred networks	Specifies whether clients can try to connect to any available IEEE 802.11 wireless networks that are within range.

Network authentication services

The IEEE 802.11-supported network authentication services provide open system and shared key authentication. Open system authentication permits any wireless device to associate with an access point. Shared key authentication requires a network key to be used. For security reasons shared key authentication is not recommended. Instead, open system authentication used in conjunction with 802.1X authentication is recommended.

Network keys

When you enable WEP, you can require that a network key be used for encryption. You can specify a key (by typing a key in the **Network key** text box when you configure the wireless connection). If you specify a key, you can also provide its location in the **Key index** text box (on the **Properties** page for **Wireless Network Connections**). Table 4.5 includes descriptions of the configuration settings for requiring network keys.

Table 4.5 Configuration Settings for Preferred Networks

Options	Comments
Networks	Lists the IEEE 802.11 wireless networks to which clients can try to connect. Use the Move Up and Move Down buttons to prioritize the list. Use the Add button to add a new wireless network. You can also edit properties of a network by using the Edit button, or use the Remove option to remove an entry from the list.
Network name (SSID)	Specifies the name for the specified wireless network. Under the IEEE 802.11 standard, the network name is also known as the Service Set Identifier (SSID).
Description	Provides a description for the specified wireless network. Use a unique description of up to 255 characters.
Wireless network key (WEP) <ul style="list-style-type: none"> • Data encryption (WEP enabled) • Network authentication (Shared mode) • The key is provided automatically 	<p>Data Encryption (WEP enabled) specifies that a network key is used to encrypt the data that is sent over the network.</p> <p>Network authentication (Shared mode) specifies that a network key be used for authentication to the wireless network.</p> <p>The key is provided automatically specifies that a network key is automatically provided for clients.</p>
This is a computer-to-computer (ad hoc) network; wireless access points are not used	Specifies whether this preferred network is a computer-to-computer ad hoc network. If this check box is not selected, this network is an access point (infrastructure) network.

IEEE 802.1X authentication

To provide user and computer identification, centralized authentication, and dynamic key management, you can enable IEEE 802.1X authentication.

You can use Group Policy to create a wireless configuration policy to configure IEEE 802.11 and IEEE 802.1X values. Table 4.6 and Table 4.7 list the wireless network policy settings that you can specify.

Table 4.6 Wireless Network (IEEE 802.11) Policy Settings

Options	Comments
Enable network access control using IEEE 802.1X	Use 802.1X authentication when you connect to an 802.11 wireless network.
EAPOL-Start message <ul style="list-style-type: none"> Do not transmit Transmit Transmit per IEEE 802.1X 	Specifies how Extensible Authentication Protocol over LAN (EAPOL)-start messages are transmitted.

Table 4.7 Wireless Network (IEEE 802.1X) Authentication Settings

Options	Comments
Parameters (seconds): <ul style="list-style-type: none"> Max start Held period Start period Authentication period 	<p>Default Max start value is 3 seconds.</p> <p>Default Held period is 60 seconds.</p> <p>Default Start period is 60 seconds.</p> <p>Default Authentication period is 30 seconds.</p>
EAP type: <ul style="list-style-type: none"> Smart card or other certificate Protected Extensible Authentication Protocol (PEAP) 	Click Settings to specify the options to use when connecting, including: using a smart card or certificate on the computer; validating server certificate; specifying which servers to connect to; Trusted Root Certification Authorities; viewing certificates; and selecting and configuring an authentication method.
Authenticate as guest when user or computer information is unavailable	Specifies whether clients attempt authentication to the wireless network as guests when user or computer information is not available.
Authenticate as computer when computer information is available	Specifies whether client computers must attempt authentication to the wireless network when a user is not logged on. The default setting is Enabled.
Computer authentication: <ul style="list-style-type: none"> With user authentication With user re-authentication Computer only 	It is recommended that you select With user re-authentication. When this option is selected, authentication is performed by using the computer credentials when users are not logged on to the computer. After a user logs on to the computer, authentication is performed by using the user credentials. When a user logs off of the computer, authentication is performed by using the computer credentials.

Creating Wireless Network Policies

You can define wireless network policies for your organization by using the Group Policy Object Editor snap-in.

► **To access Wireless Network (IEEE 802.11) Policies**

1. Open GPMC.
2. Right-click the GPO that you want to edit, and then click **Edit**.
3. In the Group Policy Object Editor console tree, click **Computer Configuration**, click **Windows Settings**, and then click **Security Settings**.
4. Right-click **Wireless Network (IEEE 802.11) Policies on Active Directory**, and then click **Create Wireless Policies**. The Wireless Policy Wizard starts.

Defining Wireless Configuration Options for Preferred Networks

By using the **Properties** page for your wireless configuration policy, you can define a list of preferred networks to use. You can use the **General** tab to specify how often to check for policy changes, which networks to access, whether to disable Zero Configuration, or automatically connect to non-preferred networks.

► **To define preferred wireless networks**

1. Open GPMC.
2. In the console tree, expand the domain or OU that you want to manage, right-click the Group Policy object that you want to edit, and then click **Edit**.
3. In the Group Policy Object Editor console tree, click **Computer Configuration**, click **Windows Settings**, and then click **Security Settings**.
4. Click **Wireless Network (IEEE 802.11) Policies**, right-click the wireless network policy that you want to modify, and then click **Properties**.
5. Click the **Preferred Networks** tab, and then click **Add**.
6. Click the **Network Properties** tab, and then in the **Name** box, type a unique name.
7. In the **Description** box, type a description of the wireless network, such as the type of network and whether WEP and IEEE 802.1X authentication are enabled.
8. In the **Wireless network key (WEP)** box, specify whether a network key is used for encryption and authentication, and whether a network key is provided automatically. The options are:
 - **Data encryption (WEP enabled).** Select this option to require that a network key be used for encryption.
 - **Network authentication (Shared mode).** Select this option to require that a network key be used for authentication. If this option is not selected, a network key is not required for authentication, and the network is operating in open system mode.
 - **The key is provided automatically.** Select this option to specify whether a network key is automatically provided for clients (for example, whether a network key is provided for wireless network adapters).

9. To specify that the network is a computer-to-computer (ad hoc) network, click to select the **This is a computer-to-computer (ad hoc) network; wireless access points are not used** check box.

► **To define 802.1X authentication**

1. Open GPMC.
2. In the console tree, expand the domain or OU that you want to manage, right-click the Group Policy object that you want to edit, and then click **Edit**.
3. In the Group Policy Object Editor console tree, click **Computer Configuration**, click **Windows Settings**, and then click **Security Settings**.
4. Click **Wireless Network (IEEE 802.11) Policies**, right-click the wireless network policy that you want to modify, and then click **Properties**.
5. On the **Preferred Networks** tab, under **Networks**, click the wireless network for which you want to define IEEE 802.1X authentication.
6. On the **IEEE 802.1X** tab, check the **Enable network access control using IEEE 802.1X** check box to enable IEEE 802.1X authentication for this wireless network. This is the default setting. To disable IEEE 802.1X authentication for this wireless network, clear the **Enable network access control using IEEE 802.1X** check box.
7. Specify whether to transmit EAPOL-start message packets and how to transmit them.
8. Specify EAPOL-Start message packet parameters.
9. In the **EAP type** box, click the EAP type that you want to use with this wireless network.
10. In the **Certificate type** box, select one of the following options:
 - **Smart card.** Permits clients to use the certificate that resides on their smart card for authentication.
 - **Certificate on this computer.** Permits clients to use the certificate that resides in the certificate store on their computer for authentication.
11. To verify that the server certificates that are presented to client computers are still valid, select the **Validate server certificate** check box.
12. To specify whether client computers must try authentication to the network, select one of the following check boxes:
 - **Authenticate as guest when user or computer information is unavailable.** Specifies that the computer must attempt authentication to the network if user information or computer information is not available.
 - **Authenticate as computer when computer information is available.** Specifies that the computer attempts authentication to the network if a user is not logged on. After you select this check box, specify how the computer attempts authentication.

For detailed information about using the wireless network policies, see “Define wireless network policies on a client computer” in Help and Support Center for Windows Server 2003.

Testing Security Policies and Rolling Out a Pilot Project

Before you deploy your security policy solution to your organization, be sure to test the configuration in a test environment and follow security policy best practices that are outlined in this chapter and in Help and Support Center for Windows Server 2003. If you have problems with your configuration, it is much easier to correct them in a non-production environment than after you deploy the configuration to your servers and clients. For more information about staging and testing Group Policy, see “Staging Group Policy Deployments” in this book.

Test customized security templates before you apply them

Do not apply the predefined security templates to production computers without first testing your customized version to make sure that the appropriate level of application functionality is maintained for the network and computer architecture.

Make sure that automatic Startup services start correctly

If you set the Startup service to start automatically, you must perform adequate testing to verify that the services can start without user intervention. For more information about setting the Startup service to start automatically, see “Configure how a service is started” in Help and Support Center for Windows Server 2003.

For more information about testing, see “Designing a Test Environment” in *Planning, Testing, and Piloting Deployment Projects* of this kit.

Additional Resources

These resources contain additional information and tools related to this chapter.

Related Information

- *Designing and Deploying Directory and Security Services* of this kit for more information about distributed security.
- “Deploying IPSec” in *Deploying Network Services* of this kit for more information about Internet Protocol security (IPSec).
- “Designing a Wireless LAN” in *Deploying Network Services* of this kit for more information about wireless networks.
- The *Networking Guide* of the *Windows Server 2003 Resource Kit* (or see the Networking Guide on the Web at <http://www.microsoft.com/reskit>).

- The *Distributed Services Guide* of the *Windows Server 2003 Resource Kit* (or see the Distributed Services Guide on the Web at <http://www.microsoft.com/reskit>) for more information about Group Policy.
- “Deploying IAS” in *Deploying Network Services* of this kit for more information about Internet Authentication Service (IAS).
- The TechNet Security link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources> for more information about Windows Server 2003 security.

Related Job Aids

- “Worksheet A.27 Using Custom Security Templates” (DMEUSE_27.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.27 Using Custom Security Templates” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.28 Selecting Predefined Security Templates” (DMEUSE_28.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.28 Selecting Predefined Security Templates” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.29 Designing Security Policy” (DMEUSE_29.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.29 Designing Security Policy” on the Web at <http://www.microsoft.com/reskit>).

Related Tools

- Group Policy Management Console
To download the GPMC tool, see the Group Policy Management Console link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Related Help Topics

For best results in identifying Help topics by title, in Help and Support Center, under the **Search** box, click **Set search options**. Under **Help Topics**, select the **Search in title only** checkbox.

- “Security Settings” in Help and Support Center for Windows Server 2003 for more information about using the security settings and security templates.
- “Internet Protocol security (IPSec)” in Help and Support Center for Windows Server 2003 for more information about using IPSec.
- “Internet Authentication Service” in Help and Support Center for Windows Server 2003 for more information about using IAS.

- “Software restriction policies” in Help and Support Center for Windows Server 2003 for more information about using software restriction policies.
- “Applying security settings through Group Policy” in Help and Support Center for Windows Server 2003 for more information about using Group Policy.
- “Creating, modifying, and assigning Active Directory-based wireless network policies” in Help and Support Center for Windows Server 2003 for more information about how to set up security policies for wireless networking.
- “Assign or unassign IPSec policy in Group Policy” in Help and Support Center for Windows Server 2003 for more information about using IPSec with Group Policy.
- “Gpupdate” in Help and Support Center for Windows Server 2003 for more information about the **gpupdate** command including full syntax.
- “Security Templates” in Help and Support Center for Windows Server 2003.
- “Security Configuration and Analysis” in Help and Support Center for Windows Server 2003.
- “Security Settings” in Help and Support Center for Windows Server 2003.
- “Local security policy” in Help and Support Center for Windows Server 2003.
- “Secedit” in Help and Support Center for Windows Server 2003.
- “Creating, modifying, and assigning IPSec policies” in Help and Support Center for Windows Server 2003.
- “Customize a predefined security template” in Help and Support Center for Windows Server 2003.
- “Predefined security templates” in Help and Support Center for Windows Server 2003.
- “Import a security template to a Group Policy object” in Help and Support Center for Windows Server 2003.
- “Define wireless network policies on a client computer” Help and Support Center for Windows Server 2003.
- “Configure how a service is started” in Help and Support Center for Windows Server 2003.

Deploying Microsoft Software Update Services



Microsoft® Software Update Services (SUS) helps you collect, approve, and distribute critical operating system patches to resolve known security vulnerabilities and stability issues. You can use these services on computers running the following operating systems: Microsoft® Windows® 2000, Microsoft® Windows® XP, and the Microsoft® Windows® Server 2003 family.

In This Chapter

Software Update Services Overview	198
Designing the Server Deployment	205
Deploying the SUS Server Component	211
Deploying Automatic Updates	226
Additional Resources	233

Related Information

- For information about Group Policy, see “Designing a Group Policy Infrastructure” in this book.
- For information about Group Policy–based software distribution and the Microsoft® Windows® Installer (MSI) packages, see “Deploying a Managed Software Environment” in this book.
- For information about Network Load Balancing (NLB), see “Deploying Network Load Balancing” in *Planning Server Deployments* of this kit.
- For an example using SUS in a simple managed environment, see “Deploying a Simple Managed Environment” in this book.

Software Update Services Overview

Prior to SUS, administrators had to continually check the Windows Update Web site for operating system patches, and then download, test, and distribute patches manually. SUS streamlines and automates these processes.

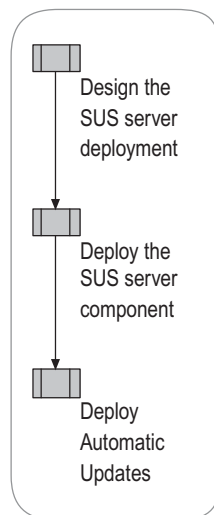
By using SUS, you can download the latest patches to an intranet server, test the patches in your operating environment, select the patches you want to deploy to specific computers, and then deploy the patches in a timely and efficient manner. SUS provides dynamic notification of critical updates to Windows-based computers, whether or not they have Internet access, and it provides a simple, automatic solution for distributing critical updates to networked clients and servers. For worksheets to assist you with the deployment of SUS, see “Additional Resources” later in this chapter.

Begin by determining the Internet connectivity, security requirements, and scale of your SUS server deployment. After deploying and testing the server configuration, deploy and configure Automatic Updates on the client computers that will connect to your servers that run SUS for critical updates. At the completion of these steps, you are ready to deploy critical patches by using SUS.

Implementing a SUS Solution

Deploying a software update solution involves determining your security and scalability needs and deciding how to stage content before distribution. You can then deploy and configure the server and client components of SUS to keep the computers in your organization updated and secure. Figure 5.1 illustrates the process of deploying SUS.

Figure 5.1. Deploying SUS



Technology Background

Many organizations do not want their computer users obtaining and installing critical or security updates from an Internet source without them being tested or approved by a system administrator. SUS allows users to install a Windows server component on an internal server running Windows 2000 Service Pack 2 (SP2) or later or Windows Server 2003. Either of these operating systems can download all critical updates and security patches as soon as they are published on the Windows Update Web site. After a patch is downloaded, you can safely test and stage its content before deploying it to production environments.

Microsoft® Systems Management Server (SMS), with the SUS Feature Pack, provides an alternative to SUS for deploying and managing software patches. For information about choosing the best patch deployment solution for your organization, see “Choosing a Security Update Management Solution,” a white paper available from the Software Update Services link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Distinguishing Patch Designations

Several tools are available for analyzing client computers and determining what patches their operating systems need. Available tools include Microsoft Baseline Security Analyzer (MBSA), Windows Update, SUS, Automatic Updates, and SMS.

MBSA MBSA is a scanning tool that runs on Windows 2000 and Windows XP operating systems to look for missing patches and service packs in Windows operating systems, Internet Information Services (IIS), and Microsoft® SQL Server™. MBSA can scan computers running Windows NT® 4.0, Windows 2000, and Windows XP operating systems. For more information about the MBSA tool, see the MBSA link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Windows Update Windows Update is a tool that scans a Windows-based computer, searching for all applicable critical, important, or moderate Windows updates. At the Windows Update Web site,, a computer running Windows can be evaluated against a known list of applicable updates to determine which updates are needed for that computer. Those updates can then be installed from this Web site. In Windows 2000, Windows XP, and Microsoft® Windows® Millennium Edition, the Automatic Updates features are added to the Windows Update program that allow you to configure computers to automatically visit Windows Update and download critical updates. For other update options, see the Windows Update link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.



Note

Automatic Updates retrieves all critical updates and Microsoft Security Response Center security updates that are classified as moderate or important.

SUS SUS is a server component that, when installed on a server running Windows 2000, allows small and medium enterprises to bring critical updates from Windows Update inside their firewalls to distribute to Windows 2000 and Windows XP computers. The same Automatic Updates component that can direct Windows 2000 and Windows XP computers to Windows Update can be directed to a SUS server inside your firewall to install critical updates.

Automatic Updates Automatic Updates scans only for critical updates, but if its server that runs SUS contains updates other than critical ones, Automatic Updates receives and applies those as well. SUS receives critical and moderate security updates.

SMS SMS 2.0 is already used by many large enterprises as the tool to distribute software updates to desktops and servers. SMS 2.0 has been extended with the SMS 2.0 Software Update Services Feature Pack to integrate with supported Microsoft scanning tools for Windows and Microsoft® Office security patches, so that entire enterprises can be scanned regularly, and the results stored by SMS as inventory. Then, the SMS administrator can automatically go to the Microsoft download center to acquire critical patches and deploy them across your enterprise.

The Microsoft Security Response Center rates the severity of an update as *critical*, *important*, *moderate*, or *low* as summarized in Table 5.1. For more information about the Severity Rating system, see the Security Response Center link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Table 5.1 Security Ratings

Rating	Definition
Critical	A vulnerability with an exploitation that can allow the propagation of an Internet worm without user action.
Important	A vulnerability with an exploitation that can result in compromise of the confidentiality, integrity, or availability of users' data, or of the integrity or availability of processing resources.
Moderate	Exploitability is mitigated to a significant degree by factors such as default configuration, auditing, or difficulty of exploitation.
Low	A vulnerability that is extremely difficult to exploit or has minimal impact.

Multiple scans performed on the same computer can show different results depending on the tool you use. MBSA finds all missing updates; Windows Update finds missing critical, important, and moderate updates; and Automatic Updates finds missing critical updates only.

You can use Automatic Updates or Windows Update in combination with MBSA. For example, after using Automatic Updates to deploy updates, run MBSA to check the update status.

Server Component

The server component of SUS is installed on Windows 2000 Server SP2 or later, or Windows Server 2003. The server running SUS synchronizes with the Windows Update Web site for operating system patches. The following discussion of SUS refers to SUS 1.0, Service Pack 1.



Note

The server component of SUS is available in English and Japanese. These languages are for the administration and installation of SUS only. Both the English and Japanese versions of SUS support clients of any locale supported by Windows.

The server component is made up of the following:

- Windows Update Synchronization Service, a synchronization service that downloads content to the servers running SUS. This service also synchronizes data among multiple servers running SUS and distribution points within the intranet.
- An IIS Web site that responds to update requests from Automatic Updates clients.
- A SUS Administration Web page.

SUS supports Windows critical updates and Windows security roll-ups only. You can apply other types of updates by using a different distribution mechanism.

Servers running SUS can be configured to synchronize content from the following sources:

- A local server running SUS that retrieves updates directly from an external Web site.
- A second-tier server on the intranet running SUS.
- A SUS content distribution point.

You can use SUS to perform staged deployments that involve multiple servers. You can configure one server in a test environment to publish updates to test clients and then review the results. If the results are satisfactory, you can configure other servers running SUS to publish those updates to the rest of your organization.

Application Compatibility

The recommended configuration is to install SUS on a dedicated server because other applications that rely on IIS might be configured in ways that are not compatible with SUS. If your organization requires that you maximize the use of each server by loading additional applications onto it, be sure that you know what changes are made to IIS when SUS is installed and how those changes might affect your other applications.

The following applications have been tested and can be safely used on the same server with SUS:

- Microsoft® FrontPage Server Extensions 2002
- Microsoft® Windows SharePoint™ Services
- Active Server Pages .NET (ASP.NET) applications

Server Component Requirements

The SUS 1.0, SP1 server component runs on Windows 2000 Server with Service Pack 2 or later, and on any operating system in the Windows Server 2003 family. It requires IIS 5.0 or later and Internet Explorer 5.5 or later.

You must install SUS on a partition that uses the NTFS file system, and the system partition on your server must also use NTFS.

The minimum configuration for a server running SUS follows:

- Pentium III 700-MHz processor or greater
- 512 megabytes (MB) of RAM
- 6 gigabytes (GB) of free disk space for setup and security packages

This configuration supports approximately 15,000 clients that use one server running SUS. The number of clients per server can be greater than this base estimate, depending on the hardware used.

SUS Client Component

The client component of SUS consists of an update to the automatic updating technology in Windows XP included with Windows Server 2003. This client component, Automatic Updates, is supported on Windows XP Professional, Windows 2000 Professional, Windows 2000 Server, and Windows 2000 Advanced Server Service Pack 2 or later.

Automatic Updates checks the local server running SUS to determine which updates are needed. It then downloads administrator-approved updates and installs the updates on client computers. The SUS administrator creates schedules for downloading updates and determines to which server each Windows-based computer connects. The rules governing the behavior of Automatic Updates are set by using Group Policy in an Active Directory environment. In a non-Active Directory environment, the administrator edits the registry directly.

Automatic Updates does not need to be installed on Windows-based computers that run Windows 2000 SP3, Windows XP Service Pack 1 or later, or a member of the Windows Server 2003 family because those operating systems already possess a SUS-compatible version of Automatic Updates. On all other intranet Windows-based servers and clients, Automatic Updates must be installed for them to connect to a server running SUS.

Automatic Updates can download packages from either a local server running SUS or from the Microsoft® Windows Update Web site (a public Web site). Typically, administrators prefer the former method because it provides a greater degree of security for clients. For more information about the Windows Update Web site, see the Windows Update link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Automatic Updates adds support for the following:

- Download of approved content from a server running SUS.
- Scheduled installations of downloaded content.
- Administrator-configurable options using either Group Policy object (GPO) or the registry.
- Ability to download critical patches to client systems where no local administrators are logged on.
- Windows 2000 operating systems.

Automatic Updates is available with the following software:

- The stand-alone setup package: MSI package.
- Windows 2000 Service Pack 3 (SP3).
- Windows XP Service Pack 1.
- Windows Server 2003 family.

Automatic Updates requires no particular hardware configuration. It can be used on any computer that runs any of the following Windows 2000 or Windows XP operating systems:

- Windows 2000 Professional, Windows 2000 Server, or Windows 2000 Advanced Server Service Pack 2 or later.
- Windows XP Professional or Microsoft® Windows® XP Home Edition.

SUS Security Features

The server running SUS contains all the synchronization service and administrative tools for managing updates. Using the Hypertext Transfer Protocol (HTTP) protocol, it responds to requests for approved updates made by the client computers connected to it. SUS can download packages from either the public Microsoft Windows Update servers or from another intranet server running SUS. During these downloads, no server-to-server authentication is carried out. All content is checked to verify that it has been correctly signed by Microsoft. Any content that is not correctly signed is not trusted and not applied.

The administration of servers running SUS is completely Web-based. You can administer the server by using either a standard HTTP connection or a Secure Sockets Layer (SSL)–enabled HTTPS connection.

Additional SUS security provisions follow:

- SUS benefits from the inherent security of NTFS because SUS must be installed on a hard disk that is formatted with NTFS.
- If a proxy password is configured, SUS stores it securely as an LSA Secret.
- Automatic Update checks the cyclical redundancy check (CRC) on each update to confirm that it was not tampered with en route.

After you run SUS Setup, you must install and configure the IIS Lockdown tool 1.0 and the Urlscan security tool 2.0 for servers running Windows Server 2000. For servers running Windows Server 2003, these tools are automatically installed and run.



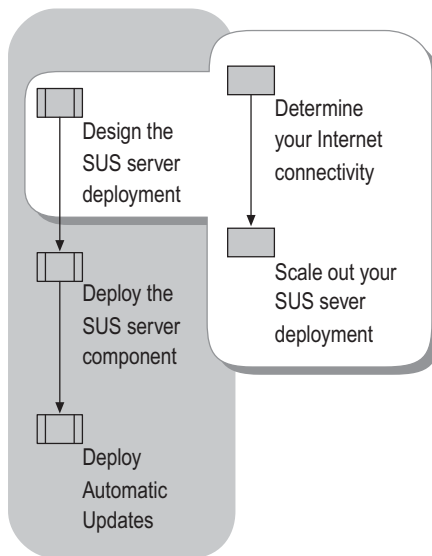
Note

For servers running Windows Server 2000, SUS does not install the latest version of the IIS Lockdown tool on your computer. For the latest version of the IIS Lockdown tool, see the IIS Lockdown tool link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources/>.

Designing the Server Deployment

Security and scalability involve the most significant decisions in designing your SUS server component deployment. You must determine your Internet connectivity and the projected scale of service. These determinations are made by viewing your current Internet connectivity policies; analyzing your security, connectivity, and scope of service needs; and then selecting the deployment model that best addresses your environment and requirements. Figure 5.2 illustrates the design process.

Figure 5.2 Designing the Server Deployment

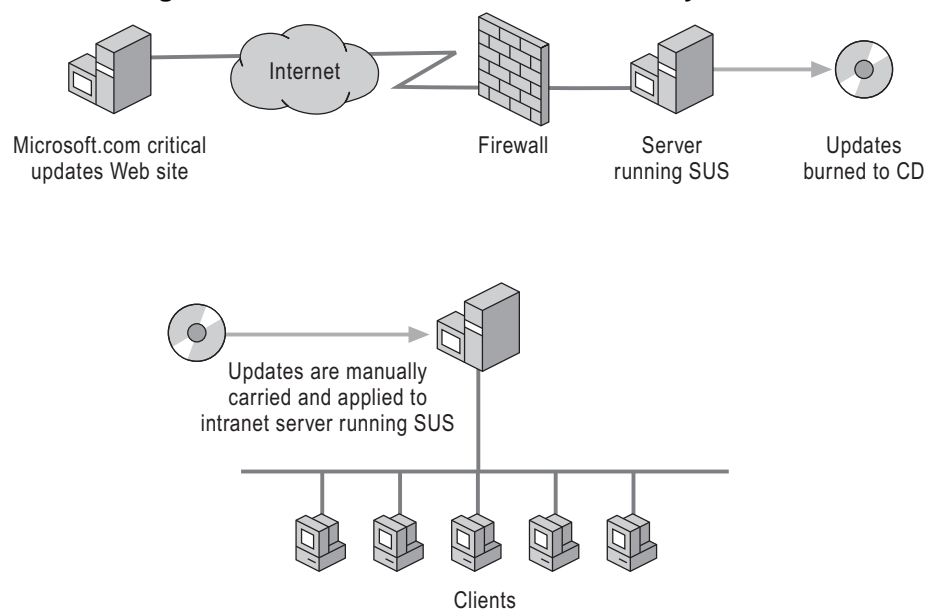


Determining Your Internet Connectivity

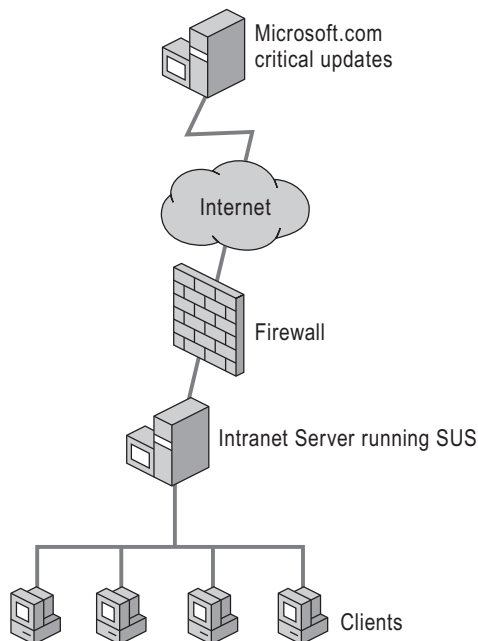
SUS provides an appropriate solution for obtaining and deploying security patches and other critical Windows patches, whether or not Windows-based networked computers in your organization are connected to the Internet. However, the existence of this connectivity does affect your SUS deployment design.

No intranet connection to the Internet If your networked Windows-based computers are not connected to the Internet, set up an internal server running SUS as illustrated in Figure 5.3. In this example, a server is created that is connected to the Internet but isolated from the intranet. After you download, test, and approve the patches on this server, you can hand-carry media to servers running SUS and to distribution points within the intranet. Although Figure 5.3 illustrates this model in its simplest form, it can be scaled to any size deployment.

Figure 5.3 SUS with No Intranet Connectivity to the Internet



Intranet connected to the Internet If your Windows-based, networked computers are connected to the Internet, you can set up a server running SUS inside the firewall of your organization, which synchronizes content directly with the external public Web site, as illustrated in Figure 5.4.

Figure 5.4 SUS with Intranet Connectivity to the Internet

Scaling Out Your SUS Server Deployment

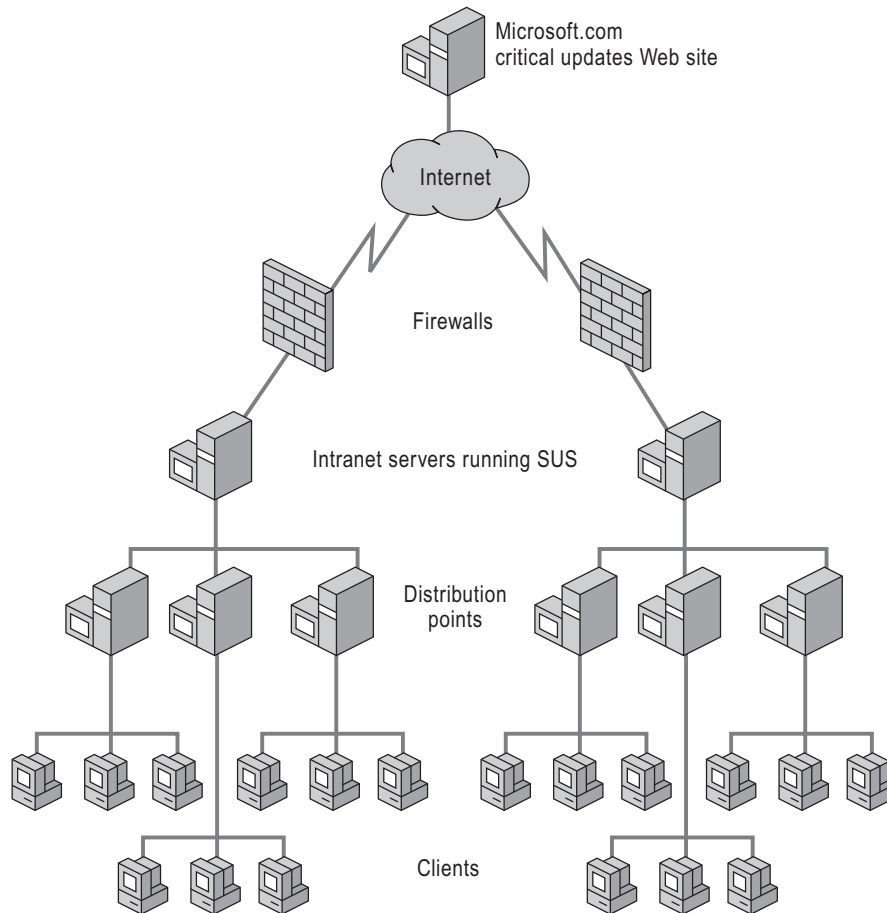
SUS deployments like those illustrated in Figures 5.3 and 5.4 can handle approximately 15,000 clients. Those models are sufficient to cover the needs of most small- or medium-size organizations. Organizations with larger or more complex networked systems, however, might require the deployment of multiple servers. For optimal performance and security, large organizations, highly secure organizations, or organizations with users spread across sites and WAN links, should deploy a multiple server model of SUS.

Some common reasons to deploy multiple servers follow:

- You have more clients to service than one server can handle efficiently.
- The clients are geographically dispersed.
- You want to avoid the risk of a single point of failure, for standard reliability concerns.
- You can scale out your SUS implementation by deploying multiple:
 - Independent servers.
 - Internally synchronized servers.
 - Internally synchronized servers enhanced with Network Load Balancing.
 - Multiple Independent Servers that run SUS.

You can deploy multiple servers that are configured so that each server is managed independently, and each server synchronizes its content to a public Web site, as illustrated in Figure 5.5. This design is an extension of the single-server model shown in Figure 5.4.

Figure 5.5 Multiple Independent Servers That Run SUS



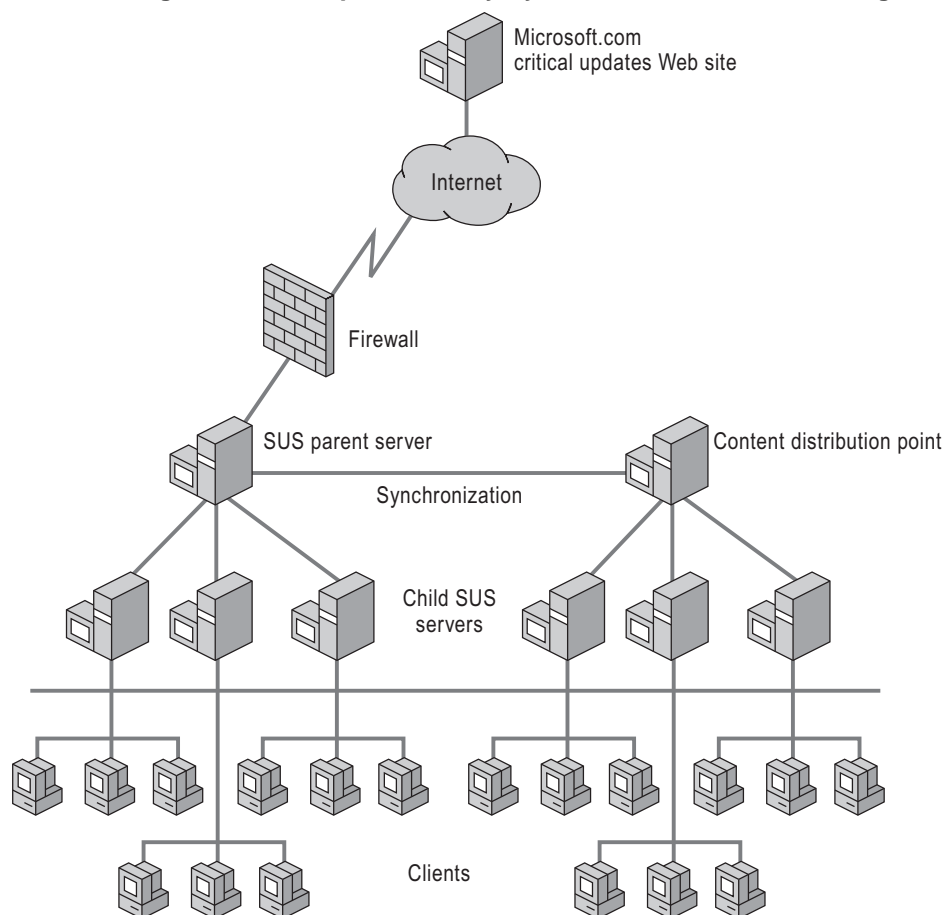
The deployment method illustrated in Figure 5.5 is appropriate for situations in which different LAN or WAN segments are managed as separate entities — a branch office, for example. It is also appropriate in cases where one server running SUS is configured to deploy patches only to clients running a certain operating system (such as Windows 2000), while another server is configured to deploy patches only to clients running another operating system (such as Windows XP). In these situations, the two servers do not need to synchronize content.

Multiple Internally Synchronized Servers Running SUS

You can deploy multiple servers running SUS that synchronize all content within your organization's intranet. In this case, one server is set up as the *parent server* — the source to which the other servers are synchronized. Additional servers running SUS — *child servers* — synchronize content from either the parent server or from a manually configured content distribution point. The child servers can perform manual or automatic synchronizations, and the synchronizations can include updates along with the list of approved updates, or updates only without the list. When applicable, the servers can be located throughout a geographically dispersed network to provide the best connectivity to all clients.

As illustrated in Figure 5.6, you can design the deployment of multiple internally synchronized servers to expose a single server to the Internet (an expanded version of Figure 5.3), or you can completely isolate your intranet from the Internet by scaling out the design as shown in Figure 5.4.

Figure 5.6 Multiple Internally Synchronized Servers Running SUS

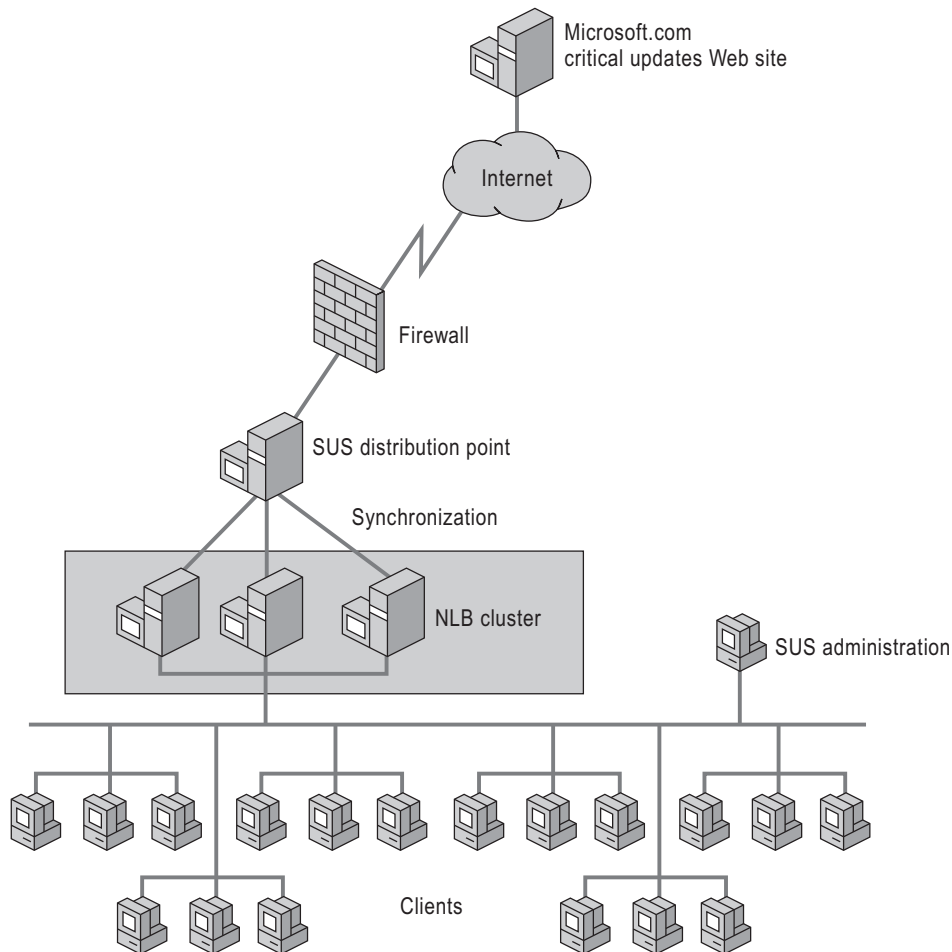


Multiple Servers Running SUS and NLB

If you have good network connectivity to a large number of clients, consider creating a central store of servers running SUS in combination with NLB as illustrated in Figure 5.7.

You can use NLB to distribute TCP/IP traffic to multiple servers running SUS. NLB partitions client requests among the servers by using one or more virtual IP addresses. Using NLB, you can configure a large number of clients to access a single location for updates and have multiple servers transparently sharing the load.

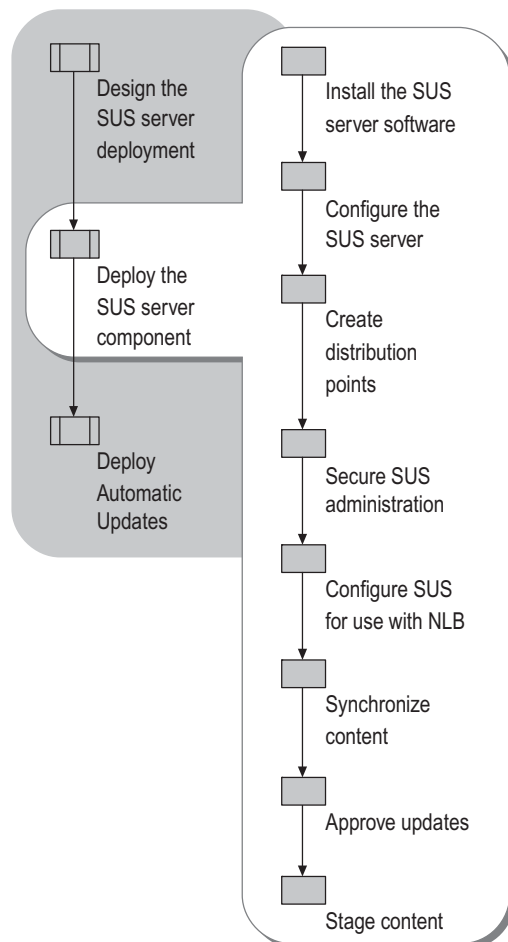
Figure 5.7 Multiple Servers Running SUS and NLB



Deploying the SUS Server Component

After you have identified the server model that best suits your needs and have installed the necessary hardware, you are ready to deploy the SUS server component. This process consists of downloading, installing, customizing, and securing the SUS server software as illustrated in Figure 5.8. After completing these tasks, you need to create any necessary additional software distribution points and child servers before testing and staging content.

Figure 5.8 Deploying the SUS Server Component



Installing the SUS Server Software

Retrieving and installing the SUS server software follows the same process whether you deploy one or multiple servers. First, install the SUS server component on the appropriate computer, keeping the default configuration. You can then configure the SUS server software. For more information, see “Configuring the SUS Server” later in this chapter.

► To retrieve and install the SUS server component from the Microsoft public Web site

1. On the Web Resources page, at <http://www.microsoft.com/windows/reskits/webresources>, click the SUS Server Component download site link.
2. On the SUS Server Component download site, follow the on-screen instructions to download and install Software Update Server.



Note

SUS setup places a shortcut for the SUS administration Web page on the **Start** menu in the Administrative Tools folder.

Configuring the SUS Server

The default server settings of the SUS server component are not applicable in all cases. On the SUS administration site, you can customize the SUS settings, identify the Domain Name System (DNS) or WINS name, and then select the appropriate content synchronization options. The default settings follow:

- Software updates are downloaded from the Windows Update Web site instead of an intranet server running SUS.
- The proxy server configuration is set to **Automatic**.



Important

SUS detects whether or not you use a proxy server. If you do, your proxy server must support auto-configuration. If it does not, you must manually configure the proxy server name and port.

- Downloaded content is stored locally.
- Content is downloaded in all languages that SUS supports.
- Patches that are approved by the SUS administrator and later updated on the public Windows Update Web site are not automatically reapproved for distribution. You must manually reapprove updated patches.

► **To change the default SUS settings**

1. On the **Start** menu, point to **Programs**, point to **Administrative Tools**, and then click **Software Update Services**.
2. In the pane on the left, click **Set Options**.
3. Select the appropriate check box to indicate whether or not you use a proxy server. If you do, configure the settings as follows:
 - If your network supports automatic proxy server configuration, select **Automatically detect proxy server settings**.
 - If your network does not support automatic proxy server configuration, select **Use the following proxy server to access the Internet**.
 - To bypass the proxy server for local addresses, select the **Bypass proxy server for local addresses** check box.
 - If your proxy server requires a user ID and password to access the Internet, select the **Use the following user credentials to access the proxy server** check box, and then enter the proxy authentication user ID and password.
 - If your proxy server requires credentials but uses basic authentication, also select the **Allow basic authentication when using proxy server** check box.



Note

When your server is configured to automatically detect proxy server settings, it also detects the absence of a proxy server.

In most Windows-based networks, client computers locate the intranet server running SUS by using the NetBIOS server name (for example, `http://SUSServer1`). If your network requires DNS, you must configure the DNS name that clients use to locate and access the server running SUS (for example: `http://susservername.domain/`). By giving the DNS name to the server, SUS returns a Uniform Resource Locator (URL) to the clients containing the DNS name.

► **To configure the DNS name**

1. Follow Steps 1 and 2 of the procedure “To change the default SUS settings.”
2. Under **Specify the name your clients use to locate this update server**, type the DNS name.

You can synchronize content on your intranet server from the external Windows Update servers, from another internal server that runs SUS, or from a distribution point.

► **To configure the option to Synchronize Content**

1. Follow Steps 1 and 2 of the procedure “To change the default SUS settings.”
2. Under **Select which server to synchronize content from**, select the text box next to your preference:

Synchronize directly from the Microsoft Windows Update servers

-Or-

To synchronize content from another intranet server running SUS or from a distribution point, select **Synchronize from a local Software Update Services server**.

3. In the text box, type the name of the server from which to synchronize content. You can enter the name in either of these formats: HTTP://<Servername> or <Server name>.

The two types of data included during the synchronization of the server running SUS are the *actual packages* and the *metadata*.

Actual packages Contain the updates. During synchronization, SUS downloads the AUCatalog.cab file. The actual packages are not downloaded unless you select the Actual packages option.

Metadata Also called *dictionary objects*, describes the available packages and their applicability. This information is located in a file named AUCatalog.cab.

If you do not download the actual packages to a local folder, they remain on the external Windows Update servers. Using this configuration, computers running the Automatic Updates client connect to the intranet server running SUS, read the list of approved packages, and then download the approved packages from the public Windows Update Web site. In this way, you can take advantage of the Windows Update servers for global scaling while maintaining local control of which updates clients install.

If you download the packages to a local folder, the packages are stored on your intranet Server running SUS. In this configuration, computers running Automatic Updates connect to the server running SUS, read the list of approved packages, and then download them directly from that server.

► **To select the location where packages reside**

1. On the **Set Options** tab of the **Software Update Services** page, select **Maintain the updates on a Microsoft Windows Updates server**.
2. Click **Save the updates to a local folder**.
3. Select the check box next to each language that you want to support.



Note

When locally hosting updates, you can add or remove supported languages at any time.

If you change the list of locales, synchronize immediately to ensure that the appropriate packages for the additional locales are downloaded. Similarly, if you modify your server running the SUS configuration from **Maintain the updates on a Microsoft Windows Update server** to **Save the updates to a local folder**, immediately perform a synchronization to download the necessary packages.

If you download content in all locales, the initial server synchronization with the Windows Update servers is approximately 600 MB of data. If you select only one or two locales to download, the initial synchronization will be approximately 150 MB.

Selecting the locales that you want to support determines only which packages are downloaded to the server running SUS. It does not determine which locales can be serviced. For example, if a computer that runs its native operating system in Japanese connects to a server that runs SUS, it retrieves a list of approved packages. If the server running SUS maintains content locally and does not support Japanese, it will fail to download the approved packages because they will not be available.

Configuring updated content approvals

In addition to the new content that is posted to the external Microsoft.com Windows Update servers, previously posted content is sometimes updated. If you approve content for distribution, and it is then updated before the distribution takes place, the content is marked on the **Approve Updates** page as **Updated**. You can customize the behavior of updated content by selecting one of the following options on the **Set Options** tab of the **Software Update Services** page:

Option 1 An approved item remains approved if it is later updated during synchronization.

Option 2 An approved item is disapproved if it is updated during a synchronization.

► To configure updated content approvals

- On the **Set Options** page, select the **Automatically approve new versions of previously approved updates** check box.

-Or-

To test packages before downloading and installing them on client computers, on the **Set Options** page, click the **Do not automatically approve new versions of previously approved updates. I will manually approve these later** check box.

Running SUS with IIS

When SUS is installed on a computer running Windows Server 2003, its setup program runs the IIS Lockdown tool 1.0 and installs and configures the Urlscan 2.0 security tool. Table 5.2 shows the settings that make IIS more secure. If SUS is installed on a computer running Windows 2000 Server, you must manually install and run these two programs separately.



Note

Windows 2000 Server running SUS does not install the latest version of the IIS Lockdown tool on your computer. Windows Server 2003 automatically installs the IIS Lockdown tool when you install IIS. For the latest version of the IIS Lockdown tool, see the IIS Lockdown tool link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Table 5.2 IIS Security Settings for Use with SUS

Option	SUS Setting
Remove Script Mappings: ASP	Enable .ASP files
Remove Script Mappings: IDQ	Disable
Remove Script Mappings: SHTML, SHTM, STM	Disable
Remove Script Mappings: IDC	Disable
Remove Script Mappings: printer	Disable
Remove Script Mappings: HTR	Disable
Remove Sample Web files	Remove
Remove Scripts Virtual Directory	Remove
Remove MSDAC virtual directory	Remove
Disable WebDAV	Disable WebDav
Prevent IIS anonymous user from executing system utilities	Prevent
Prevent IIS anonymous user account from writing Web content	Prevent

Because IIS 5.0 runs in a secure mode by default, IIS Lockdown is not applied when you install SUS on computers that run Windows Server 2003. However, the SUS setup program sets a property in the IIS metabase to enable asp.dll. The following *ISAPIRestrictionList* setting disables all script mappings except asp.dll.

```
ISAPIRestrictionList: = "0", "asp.dll"
```


In addition to disabling script mappings, the changes listed in Table 5.3 are made to the IIS metabase during SUS setup. The change occurs whether the server operating system is Windows 2000 or Windows Server 2003.

Table 5.3 IIS Metabase Changes

Property	Value	Result
w3svc/AspProcessorThreadMax	1	Ensures that IIS does not start more than one thread per process
w3svc/AspThreadGateEnabled	True	Throttles the number of threads based on CPU usage

At the end of its setup routine, SUS stops any Web site running on that server.

For security purposes, SUS disables several ISAPI handlers when SUS is installed on the host IIS server. This can disable existing functionality for sites that rely on any of the following technologies:

- ASP.NET
- FrontPage Server Extensions
- Windows SharePoint Services

If you have Web sites that rely on any of these technologies, you must re-enable the necessary *ISAPI handlers* after SUS setup is completed.

For FrontPage Server Extensions and Windows SharePoint Services, enable the following ISAPI handlers:

- admin.dll
- fpadmdll.dll
- author.dll
- owssvr.dll
- shtml.dll

► **To enable an ISAPI handler**

1. Start the IIS snap-in, found in the **Administrative Tools** folder on the **Start** menu.
2. Right-click the server node, and then click **Security**.
3. To view the **Enable request handles** page, click **Next** one or more times.
4. Under **ISAPI Handlers**, select each ISAPI handler that you want to enable, and then complete the wizard.

Creating Distribution Points

When you install a server that runs SUS, a distribution point is created on that server. When you synchronize the server with a parent server or with an external Web site, all the content on the Web site is downloaded to the distribution point. If new updates are downloaded, this distribution point is updated during every synchronization. During Setup, the distribution point is created in a virtual root (Vroot) named /Content.

If you choose to maintain content on the public Web site instead of downloading the patches to the local server running SUS, this distribution point is empty except for the AUCatalog.cab file. AUCatalog.cab defines the updates that have been approved for deployment to clients.

You can also create a distribution point on a server that is not running SUS. Such a server must be running IIS 5.0 or later. You can download and test packages on servers running SUS, and then download approved and tested packages to distribution points for client access.

If your SUS design includes distribution points, perform the following tasks to create a distribution point:

1. Confirm that IIS is present.
2. Create a folder named \Content.
3. Copy all of the following items from the source server running SUS to the newly created \Content folder:
 - <root of the SUS Web site>\Aucatalog1.cab
 - <root of the SUS Web site>\Aurtf1.cab
 - <root of the SUS Web site>\approveditems.txt
 - All the files and folders under the \Content\cabs
4. Create an IIS Vroot called http://<Servername>/Content that points to the \content folder.

►
point

To set up SUS to synchronize from a manually created content distribution

1. On the Administration Web site (http://<Your servername>/SUSAdmin), click **Set Options**.
2. Under **Select which server to synchronize content from**, click **Synchronize content from a local server running Software Update Services**.
3. In the text box, enter the name of the server (<Servername> or http://<Servername>) that has a manually created content distribution point from which you want to synchronize.

Securing SUS Administration

You can administer a server that runs SUS by running Internet Explorer from a remote computer. By default, all administration is done over HTTP by using the following URL: `http://<servername>/SUSAdmin`. Only users with local administrator credentials on the server on which SUS is installed can use the SUS administration Web site.

By using HTTP, you can send all communications in plaintext over the network without any encryption during your administrative session. You have two choices for securing SUS administration:

- Administer the server locally only, and never from a remote computer.
- Use secure HTTPS/SSL for server administration.

Before using HTTPS for secure remote administration, you must obtain and install a valid digital certificate for server authentication from your organization. For more information about installing digital certificates, see “Installing and configuring a certification authority” in Help and Support Center for Windows Server 2003, or talk to the security administrator in your organization.

► **To turn on HTTPS for secure remote administration**

1. Start the IIS MMC snap-in.
2. On the SUS **Properties** page, set the SSL port to 443.
3. On the **Directory Security** tab, start the Web Server Certificate wizard by clicking **Server Certificate**.
4. Follow the wizard instructions to assign the digital certificate for SSL authentication for SUS.



Important

Store the digital certificate for SSL in the local computer store of the server that you want to administer.

► **To enable SSL for the SUS folders**

1. Right-click the administration folder (\autoupdate\administration) in the navigation pane, and then click **Properties**.
2. Click the **Directory Security** tab, and then click **Edit**.
3. Select the **Require Secure Channel (SSL)** and the **Require 128-bit Encryption** check boxes.
4. Repeat steps 1 and 2 for each of the following additional folders:
 - \autoupdate\dictionaries
 - \shared\content\EULA



Note

The \Content\EULA folder does not appear until SUS performs at least one successful synchronization.

Configuring SUS for Use with NLB

If your deployment consists of multiple servers in a central location, NLB can help balance the flow of incoming and outgoing TCP/IP traffic between these servers and their clients. To configure this load-balancing model, perform the following tasks:

1. Create a manually configured content distribution point. For more information, see “Creating Distribution Points” earlier in this chapter.
2. Make sure that this content distribution point contains content for all the locales you need to support for all clients.
3. Configure each server running SUS to do the following:
 - Store content locally.
 - Synchronize from the appropriate content distribution point.
 - Synchronize the list of approved items from the same content distribution point.
4. Install and configure NLB on each server that is part of the cluster. For more information about deploying NLB, see “Deploying Network Load Balancing” in *Planning Server Deployments* in this kit.
5. Configure your clients to point to this cluster for its updates by using either the cluster’s virtual IP address or its DNS or WINS name.

Running NLB in unicast mode

When running NLB in unicast mode with a single network card in each server, keep the following in mind:

- Each server in the NLB cluster synchronizes content from the manually configured content distribution point.
- The NLB service determines which host in the cluster will respond to each client request.
- You cannot access resources on one server from another server in the cluster.
- To administer any servers in the cluster, you must be at the console of that server, or use a remote client outside of the cluster.



Important

It is recommended that you install NLB in Unicast mode with a single network interface card (NIC) in each server because all the servers involved are on the same Intranet.

After you install and configure the NLB service on each server running SUS, you have a virtual IP address that you can use to access the cluster. You can register this IP address with a friendly name on your DNS or WINS servers.

Synchronizing Content

A server running SUS can be synchronized with the public Windows Update servers, with another server running SUS, or with a SUS distribution point.

Synchronizing from another Windows Update corporate server or distribution point is useful if the following conditions exist:

- You have multiple servers running SUS, and you do not want all of them to go to the Internet to synchronize content.
- You have physical sites that do not have Internet access.
- You want to test content in a controlled environment and put the testing content on a distribution point from which the production servers running SUS synchronize.



To synchronize content immediately

1. On the Software Update Services Administration page, in the navigation pane on the left, click Synchronize server.
2. Click **Synchronize now**.

- **To view information about your synchronizations and downloaded updates**
 - In the navigation bar on the left, click **View synchronization log**.
- **To create a new schedule, modify an existing schedule, or turn off the current schedule**
 1. In the navigation bar on the left, click **Synchronize server**.
 2. In the **Synchronization Schedule dialog box**, select the settings you want.

Synchronizing the List of Approved Packages

In addition to synchronizing content, Software Update Services can synchronize the list of approved packages either with another server that runs SUS or with a SUS distribution point. If you have multiple servers running SUS or distribution points or both, you can approve a list of packages on a parent server. Child servers and distribution points then synchronize to the parent server for retrieval of the current list of approved packages. In this case, the list of approved items cannot be modified on the child server or distribution point. All changes to the approved list must occur on the parent server.

- **To synchronize the list of approved items with the content**
 - On the **Set Options** page of the Software Update Services Administration page, select the **Synchronize list of approved items updated from this location (replace mode)** check box.
-

Approving Updates

As an administrator, you have complete control over which updates are downloaded to which client computers. This control is offered from the SUS Administration page.

For each item on the **Approval Page**, SUS displays the item status in the right corner of the item description (see Table 5.4).

Table 5.4 Update Types

Status	Explanation
New	The update that was recently downloaded has not been approved and will not be offered to any clients that query the server.
Approved	The update has been approved by an administrator and is available to clients that query the server.
Not Approved	The update has not been approved and is not available to clients that query the server.
Updated	The update has been changed during a recent synchronization.
Temporarily Unavailable	One of the following conditions exists: <ul style="list-style-type: none"> • The associated update package is not available. • A dependency required by the update is not available.

► **To obtain more information about a particular update**

1. On the navigation pane on the left, click **Approve updates**.
2. Under the update name, click **Details**.
3. Select the information you want from the list, which includes the following:
 - The .cab files associated with the package.
 - The locale for each .cab file.
 - The platform for each .cab file.
 - A link to the actual .cab file that was used to install the package and any command-line setup options necessary to install the package.
 - A link to the **Read more** page about the update.

► **To approve or disapprove updates**

1. On the navigation bar on the left, click **Approve updates**.
2. Select the updates that you want to distribute to your clients.
3. Click **Approve**.

-Or-

To disapprove updates, clear the check boxes next to all updates, and then click **Approve**.

When you disapprove the updates, current packages are not available to any of your clients. You are notified whether the approval is successful. For more information about the updates you have approved, click **View approval log** in the left navigation bar.

Reviewing Server Actions and Server Functionality

The synchronization and approval logs are stored in XML files in a folder accessible to administrators on the server running SUS. New information is continually appended to these files, so it is recommended that you regularly remove out-of-date information.

You can check the functionality of the server running SUS by using the Monitor Server page, which is accessible on the administrative user interface. This page is stored in RAM and needs to be occasionally refreshed.

The synchronization service also generates an Event Log message whenever any of the following events occurs:

- The server performs a synchronization.
- The synchronization service encounters a major error.
- The list of approved updates changes.

Reading the Approval Log

An approval log is maintained on each server running SUS to track the content that has been approved or not approved. The approval log contains the following information:

- A record of each time the list of approved packages was changed.
- The list of items that changed.
- The new list of approved items.
- A record of who made the change — either the server administrator or the synchronization service.

You can access the log from the left navigation pane in the administrative user interface, or you can access it directly by using any text editor. The file name is `history_Approve.xml`, and it is located in the SUS installation folder under `\VRoot\AutoUpdate\Administration`.

Reading the Synchronization Log

SUS maintains a synchronization log on each server running SUS to track the content synchronizations it has performed. You can access the log from the SUS Administration Web page, or you can access this file directly by using any text editor. The file name is `historySync.xml`, and it is located in the SUS installation folder under `\VRoot\AutoUpdate\Administration`. This synchronization log contains the following:

- The time that the last synchronization occurred.
- Success and failure information for the overall synchronization operation.
- Time of the next synchronization if scheduled synchronization is enabled.
- The update packages that have been downloaded or updated since the last synchronization.
- The update packages that failed synchronization.

► To read the Synchronization Log

- In the navigation bar on the left, click **View synchronization log**.

Staging Content

Before you distribute patches onto your organization's production computers, it is recommended that you test them. Before deploying the client component of SUS, you need to have a staging and testing plan in place. You have two options for staging content.

Option one for staging content

1. Set up one server running SUS for testing.
2. Download and test the content on the test server running SUS and on at least one test client for each operating system.
3. After you test the content, approve it on a production server running SUS.

The production server synchronizes with the public Web site for the approved content, and the clients retrieve the approved patches during their next polling cycle.



Caution

The first staging option incurs the risk of approving content that is changed before the clients actually begin downloading it. The second option prevents this risk because it copies content as well as the approved list to the distribution point server.

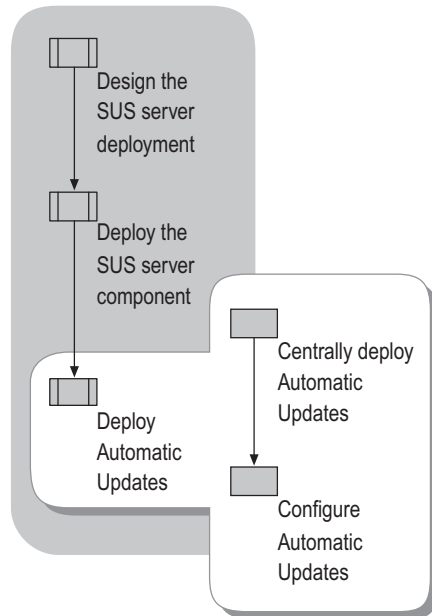
Option two for staging content

1. Perform steps 1 and 2 in the "Option One for Staging Content" procedure.
2. After you test the content, copy the list of approved items and the tested content to a distribution point.
3. Configure the production server running SUS to download the content and the list of approved items to clients and child servers from the distribution point.
4. Download the content.

Deploying Automatic Updates

SUS requires the installation of Automatic Updates (see Figure 5.9), a feature that allows Windows-based computers to receive content from the SUS server. There are several ways you can deploy Automatic Updates to your client computers, depending on your operating environment. After you deploy Automatic Updates, you can centrally control its configuration on the clients.

Figure 5.9 Deploying Automatic Updates



The simplicity of the MSI setup for Automatic Updates makes it the preferred method for updating computers that run Windows 2000 and Windows XP. If your client computer is running Windows 2000 SP2 or Windows XP, deploy Automatic Updates as follows: On the Software Update Services Client Web site, follow the on-screen instructions to download and run the Automatic Updates client software.



Note

You can also deploy the MSI package to clients centrally. For more information about centralized deployment, see “Deploying Automatic Updates” later in this chapter.

Methods of receiving Automatic Updates for clients running operating systems other than Windows 2000 SP2 or Windows XP follow:

- Install Windows 2000 SP3.
- Install Windows XP SP1.
- Install Windows Server 2003.

Centrally Deploying Automatic Updates

Prior to centrally deploying Automatic Updates, create a Group Policy software distribution point that contains the WUAU22.msi file for clients to access.

After creating the required distribution point, you can centrally control Automatic Updates deployments by using any of the following methods: Group Policy Software Distribution, SMS, or a logon script.

Group Policy Software Distribution Use this method if your network uses Active Directory and Windows 2000 or later.

SMS Use this method if you are running SMS on your network.

A logon script Use this method if Active Directory is not part of your operating environment. A logon script is appropriate for users with local computer administrator permissions.

Several methods are available for deploying Automatic Updates. Select the option that best suits your environment.

Deploying Automatic Updates by using Group Policy for Active Directory environments

1. Create a Group Policy object (GPO).
2. Edit the GPO you just created.
3. Under **Computer Configuration** or **User Configuration**, expand **Windows Settings**.
4. Double-click **Scripts**.
5. Double-click the type of script you want to deploy (**Startup/Shutdown** for computer, or **Logon/Logoff** for user.)
6. Create a script that contains the following semantics:
 - If %windir%\system32\wuaueng.dll is earlier than version 5.4.3630.11, write the script so that it only installs wuau22.msi.

This can be done using VBScript, using the GetFileVersion method on the Scripting.FileSystemObject object. Be sure to allow sufficient time for the policies to replicate throughout the domain, and then restart the client computers.

When you restart the client computers, the packages are installed, and the policies are processed. Because the application is installed on the local computers, be sure that authenticated users have the appropriate permissions to open source folders.

Deploying Automatic Updates client by using Self-Update

Automatic Updates self-upgrades when a newer version is posted on the server that it checks for updates. Each time Automatic Updates checks the public Web site or internal server that runs SUS for updates, it also checks for a newer version of Automatic Updates.

► To confirm that the Updated Automatic Updates installed successfully

1. In the **Run** dialog box, type: %windir%\system32\
2. Right-click **Wuaueng.dll**, and then click **Properties**.
3. On the **Version** tab, confirm that the version number is 5.4.3630.11 or higher.

Configuring Automatic Updates

Automatic Updates downloads critical updates based on the configuration options that the user selects by using the Automatic Updates tool in Control Panel, or by reading the policy settings that an administrator configures.

If you configure Automatic Updates to notify the user of updates that are ready to be downloaded, it sends the notification to the system Event Log and to a logged-on administrator of the computer. If no administrator is logged on, Automatic Updates waits for an administrator to log on before offering the notification.

Every 22 hours minus a random offset, Automatic Updates polls the server running SUS for approved updates. If any new updates need to be installed, the client downloads them.

You can manipulate the notification options as follows:

- If Automatic Updates is configured to notify the user of updates that are ready to install, the notification is sent to the system Event Log and to the notification area of the server running SUS.
- When a logged-on administrator clicks the notification area icon, Automatic Updates displays the available updates to install. The user must then click the **Install** button for the installation to proceed. A message appears if the update requires the computer to be restarted to complete the update. Until the system is restarted, Automatic Updates cannot detect additional updates.
- The **Remind Me Later** button provides a way for the installation to be deferred. The options are **30 minutes**, **1 hour**, **2 hours**, **4 hours**, **8 hours**, **tomorrow**, and **in 3 days**.

If Automatic Updates is configured to install updates on a set schedule, applicable updates are downloaded and marked as ready to install. A logged-on administrator is notified by the notification-area icon, and an event is logged to the system Event Log. This indicates that the updates can be installed. If the user clicks the notification, a dialog box appears in which the **Remind Me Later** option is unavailable.

At the scheduled day and time, Automatic Updates installs the update and restarts the computer (if necessary), even if there is no local administrator logged on. If a local administrator is logged on, Automatic Updates displays a warning that an installation is about to begin.

If it is required to restart the computer, and any user is logged on, a similar countdown dialog box is displayed, warning the logged-on user about the impending restart.

After the new updates are downloaded, Automatic Updates polls the server running SUS again for the list of approved packages to confirm that the packages it downloaded are still valid and approved. This means that if an administrator removes updates from the list of approved updates while Automatic Updates is downloading updates, only the updates that are still approved are actually installed.

Administrative Methods for Configuring Automatic Updates

Group Policy is the preferred method for configuring your client computers because of its precise control. You can also set policies by using Windows NT 4.0 System Policy or by editing the registry directly.

Administrator-defined configuration options driven by Group Policy always take precedence over user-defined options. Automatic Updates options in Control Panel options are disabled on the target computer when administrative policies have been set by the administrator.

Applying Group Policy in an Active Directory Environment

In a test environment, apply Group Policy settings by using the Local Group Policy object. In production environments, it is typically more efficient to set policies at the organizational unit (OU) or domain level. Be aware that some Group Policy settings have an effect on other settings, such as removing access and links to Windows Update features.

Remove access to use all Windows Update features If this setting is enabled, Automatic Updates is disabled for that logged-on user. Because this policy is a user-based value, it makes a local administrator appear as a nonadministrator. With this policy enabled, Automatic Updates still runs, and scheduled installations can still occur. This setting is available only in Windows XP. Use this policy if you do not want some users to receive updates from SUS.

Remove links and access to Windows Update If this setting is enabled, Automatic Updates receives updates from your server that runs SUS. Users who have this policy set cannot get updates from a Windows Update Web site that you have not approved on your server that runs SUS. If this policy is not enabled, the Windows Update icon remains on the **Start** menu for local administrators to visit the Windows Update Web site. Local administrative users can use it to install unapproved software from the public Windows Update Web site. This happens even if you have specified that Automatic Updates must get approved updates from your server that runs SUS.

► To configure the behavior of Automatic Updates clients by using Group Policy

1. Using the Group Policy Management Console (GPMC), create a new GPO or edit an existing GPO to which you want to add this setting.
2. Expand **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **Windows Update**.
3. On the Windows Update template, click **Configure Automatic Updates**.
4. Select one of the following options:
 - **Notify for download and notify for install.** This option notifies a logged-on administrative user prior to the download and prior to the installation of the updates.
 - **Auto download and notify for install.** This option automatically begins downloading updates and then notifies a logged-on administrative user prior to installing the updates.
 - **Auto download and schedule the install.** Typically, if Automatic Updates is configured to perform a scheduled installation, the recurring scheduled installation day and time are also set.

► **To redirect Automatic Updates to a server running SUS**

1. In the details pane of the Group Policy MMC snap-in, click **Specify Windows Update Server**.
2. In the text box, type the name of the server that runs SUS.

In addition to specifying a server, you can also identify a computer to which you want Automatic Updates to send statistics. The statistics server must be running IIS. The statistics sent to the server are stored in the IIS logs. The same server can host both SUS and the statistics.

If the policy is disabled or not configured, Automatic Updates gets its updates from the public Windows Update service.

See the **Explain** tab for the **Reschedule Automatic Update** scheduled installations and the **No auto-restart** for scheduled Automatic Update installation options, to see how those settings best suit your environment.

Configuring Automatic Updates in a Non-Active Directory Environment

In a non-Active Directory environment, you can configure Automatic Updates by modifying the registry by using the following methods:

- Editing the registry directly by using the registry editor Regedit.exe.
- Centrally deploying these registry entries by using System Policy in Windows NT 4.0 style.



Caution

Do not edit the registry unless you have no alternative. The registry editor bypasses standard safeguards, allowing settings that can damage your system, or even require you to reinstall Windows. If you must edit the registry, back it up first, and then see the Registry Reference on the Windows Server 2003 Deployment Kit companion CD or at <http://www.microsoft.com/reskit>.

The registry entries for the Automatic Update configuration options are located in the following subkey:

HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU.

The keys and their value ranges are listed in Table 5.5.

Table 5.5 Automatic Updates Configuration Registry Keys

Entry Name	Value Range and Meanings	Data Type
NoAutoUpdate	Range = 0 1 0 = Automatic Updates is enabled (default), 1 = Automatic Updates is disabled	Reg_DWORD
AUOptions	Range = 2 3 4 2 = notify of download and installation, 3 = automatically download and notify of installation, and 4 = automatic download and scheduled installation. All options notify the local administrator	Reg_DWORD
ScheduledInstallTime	Range = n; where n = the time of day in 24-hour format (0-23)	Reg_DWORD
UseWUServer	Set this to 1 to enable Automatic Updates to use the Windows Update server as specified in WU Server.	Reg_DWORD
ScheduledInstallDay	Range = 0 1 2 3 4 5 6 7 0 = Every day; 1 through 7 = the days of the week from Sunday (1) to Saturday (7).	Reg_DWORD
RescheduleWaitTime	Range=n; where n=time in minutes (1-60).	Reg_DWORD
NoAutoRebootWithLoggedOnUsers	0 to 1; set this value to 1 if you want logged on users to choose whether or not to reboot their system.	Reg_DWORD

To specify the server running SUS that you want your clients and servers to connect to for their Windows updates, you need to add two entries to the registry in the subkey
HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate. For the required entries, see Table 5.6:

Table 5.6 Automatic Updates Server Selection Registry Keys

Entry Name	Values	Data Type
WUServer	The HTTP name for the Windows Update intranet server (for example, http://intranetsus).	Reg_SZ
WUStatusServer	The HTTP name for the Windows Update intranet server (for example, http://intranetsus).	Reg_SZ

Additional Resources

These resources contain additional information and tools related to this chapter.

Related Information

- The Microsoft Security Response Center link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources> for more information about security ratings.
- The Software Update Services link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources> for more information about Software Update Services.
- The Software Update Services Overview white paper, available from the Software Update Services link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources> for more information about how SUS can improve security for your organization's Windows-based computers.
- The SMS Product Information link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.
- The Windows Update Roadmap link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources> for information about the differences between Windows Update, Windows Update Catalog, and Software Update Services.
- The Software Update Services Download Site link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources> for more information about downloading Software Update Services software.
- "Choosing a Security Update Management Solution," a white paper available from the Software Update Services link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>, for information about choosing the best patch deployment solution for your organization.
- The Software Update Services Deployment White Paper link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources> for more information about troubleshooting SUS deployment.

Related Tools

- E-mail Notification Service

The E-mail Notification Service tool provides a free notification service that Microsoft uses to send information to subscribers about the security of Microsoft products. For more information about the E-mail Notification Service tool, see the E-mail Notification Service link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

- IIS Lockdown

The IIS Lockdown tool provides templates for the major IIS-Microsoft products. The IIS Lockdown tool works by turning off unnecessary features, thereby reducing the attack surface available to attackers. The IIS Lockdown tool must be downloaded separately for servers running Windows 2000 Service Pack 2 (SP2), but it is built in to Windows Server 2003. For more information about IIS Lockdown, see the IIS Lockdown tool link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

- Microsoft Baseline Security Analyzer

The Microsoft Baseline Security Analyzer (MBSA) tool provides a streamlined method to identify common security misconfigurations. MBSA 1.1 includes a graphical and command-line interface that can perform local or remote scans of Windows operating systems. For more information about the MBSA tool, see the MBSA link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

- Windows Update

Windows Update is an online extension of Windows that provides scanning software and download opportunities for Windows operating system patches. For more information about Windows Update, see the Windows Update link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Related Help Topics

For best results in identifying Help topics by title, in Help and Support Center, under the **Search** box, click **Set search options**. Under **Help Topics**, select the **Search in title only** checkbox.

- “Installing and Configuring a Certification Authority” in Help and Support Center for Windows Server 2003.

Related Job Aids

- “Worksheet A.31 Scaling a SUS Deployment” (DME_USE31.doc) on the *Microsoft® Windows® Server 2003 Deployment Kit* companion CD (or see “Worksheet A.31 Scaling a SUS Deployment” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.32 Deploying the Server Component” (DMEUSE_32.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.32 Deploying the Server Component” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.33 Deploying Automatic Updates” (DMEUSE_33.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.33 Deploying Automatic Updates” on the Web at <http://www.microsoft.com/reskit>).

Migrating User State

6

When you move client computers to the Microsoft® Windows® XP operating system from earlier versions of Windows, it is important to save and then restore user data and settings. This process is known as *migrating user state*. By carefully planning and implementing user state migration, you help conserve IT staff time, preserve important data, scale the migration as needed, and minimize costs while maintaining user productivity and workplace morale.

In This Chapter

Overview of Migrating User State	236
Choosing a User State Collection Method	241
Identifying Migration Content	248
Creating a Detailed Migration Plan	251
Testing Your Migration Process	258
Additional Resources	260

Related Information

- For information about using Remote Installation Services (RIS), see “Designing RIS Installations” in *Automating and Customizing Installations* of this kit.
- For information about scripting in a Microsoft® Windows® Server 2003 operating system environment, see the Windows Deployment and Resource Kits Web site at <http://www.microsoft.com/reskit>, or see the MSDN Scripting Clinic link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Overview of Migrating User State

Any time that you perform a new installation of Windows XP on a client workstation, you should migrate user state to ease users into the new system and maintain user productivity. *User state* consists of *user data* — the files that users create and need to do their jobs — along with *user settings* containing application-specific and user-specific information. Additionally, application settings supply the user with links, menus, and other information that can be essential for their productivity.

If user state is not migrated, an organization can accrue costs as users spend production time reconfiguring their applications and other settings. Organizations must evaluate the cost/benefits ratios for migrating various types of items. They must understand the security issues related to migration and be sure to educate users about what to expect before and after the migration.

The way that you choose to deploy Windows XP affects your user state migration plan. Ideally, an organization can perform either a parallel or a wipe-and-load deployment, restoring collected user state to a clean environment.

The method that you use to collect and restore user state is critical to the success and efficiency of your user state migration. To avoid the high migration cost of a strictly manual migration, an organization can:

- Partially script the migration, leaving nonstandard items to the discretion of the individual user or IT staff.
- Use migration tools that automate the migration of common settings but allow customization.
- Create its own custom tools.

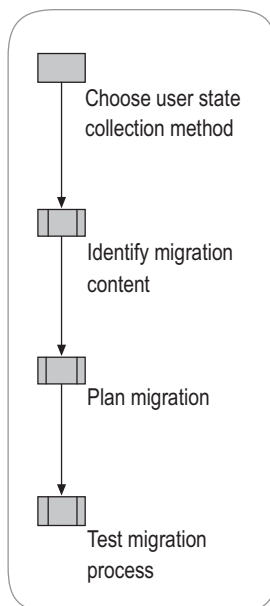
The degree to which an organization should automate user state migration depends on these and a variety of other factors, including the number of users to be migrated and how widely dispersed they are; how centralized the organization's IT effort is; the degree to which users share a common desktop, folder hierarchy, and computing requirements; the IT expertise available to assist in and support the migration; and whether the deployment involves simultaneous domain migration.

Before you begin planning a user state migration, identify the computers on which you will deploy Windows XP, and determine the appropriate deployment method for each computer. When you complete this process, you will be ready to deploy Windows XP, with a complete, tested plan for migrating user state during the system deployment and a schedule for the migration. For worksheets to assist you with the deployment of migrating user state, see "Additional Resources," later in this chapter.

User State Migration Process

Proper planning is essential for a successful user state migration. Before creating a detailed migration plan, identify the best methods for collecting, storing, and restoring user state data and decide which user data and settings to migrate. After making these decisions, prepare a migration plan that addresses storage and security requirements; potential registry, drive, and domain changes; scheduling; and the education of users. Then test your migration process before embarking on a large-scale migration. Figure 6.1 shows the process for planning a user state migration.

Figure 6.1 Migrating User State



Tools Used in the Migration Process

Some large organizations develop their own migration tool. This frequently provides an excellent migration experience for the user, because the tool is customized to the specific environment. Such a tool can capture and restore user settings and files. Adjustments can be made quickly when new applications are deployed or bugs are found.

Typically, this option requires a significant investment in development time. If your organization does not have personnel who can create a migration tool, the cost of hiring programmers to create one might be prohibitive. Even if you do have programmers on staff, compare the cost of tool development with the migration costs of other available methods.

Many tools currently available from vendors can collect and restore most necessary settings and are extensible to include additional application settings. These tools often provide multiple types of rules to specify which files to migrate. However, while fairly thorough, such tools are not targeted to your specific environment, and their initial cost can be high.

Microsoft provides two tools designed specifically for migrating user state in a Windows environment:

- The Files and Settings Transfer Wizard
- The User State Migration Tool (USMT)

Both tools automate the migration of basic application, operating system, and user settings, as well as user data, and both support customization.

Files and Settings Transfer Wizard

The Files and Settings Transfer Wizard is a Windows XP accessory, available in **Systems Tools**. (On the **Start** menu, point to **All Programs**, **Accessories**, **System Tools**, and then click **Files and Settings Transfer Wizard**.) The wizard enables users to migrate personal display properties, folder and taskbar options, and Internet browser and mail settings, as well as specific files or entire folders (such as **My Documents**, **My Pictures**, and **Favorites**) from their old computer to their new one without any manual configuration.

Designed for home users and small office users, the Files and Settings Transfer Wizard is also useful in a corporate network environment, for employees who get a new computer and need to migrate their own files and settings without the support of an IT department or Help desk. For information about using the Files and Settings Transfer Wizard, see Help and Support Center for Windows XP.

User State Migration Tool (USMT)

Designed for IT administrators who are performing large deployments of the Microsoft® Windows® XP Professional operating system in a corporate environment, USMT provides the same functionality as the Files and Settings Transfer Wizard, but on a large scale targeted at migrating multiple users. USMT gives administrators precision in configuring unique settings, such as making user-specific modifications to the registry. The tool is included on the Microsoft® Windows® Server 2003 operating system CD in the \ValueAdd\Msft\USMT folder.

USMT uses the following files in collecting and migrating user data and settings:

- Scanstate.exe collects user state.
- Loadstate.exe restores user state.
- Migapp.inf determines which application settings are migrated.
- Migsys.inf determines which operating system settings are migrated.
- Miguser.inf determines which user settings are migrated.
- Sysfiles.inf defines files that *must not* be migrated despite any other rules. These are operating system files that will conflict with the newer version of the files in Windows XP. The SysFiles.inf file should not be modified except to add more files to the list of files that never migrate under any circumstances.

These files are shipped with Windows XP in the ValueAdd\Msft\USMT folder.

Table 6.1 and Table 6.2 list the file types, folders, settings, and system components that are migrated by default using USMT. (See also the Inf Commands.doc file included on the Windows Server 2003 operating system CD in the \ValueAdd\Msft\USMT folder.)

Table 6.1 File Types and Folders Migrated by Default by USMT

File Types Migrated			Folders Migrated
.doc	.xl?	.dif	Desktop
.dot	.csv	.ppt	My Documents
.rtf	.iqy	.pps	My Pictures
.txt	.dqy	.pot	Favorites
.mcw	.oqv	.sh3	Cookies
.wps	.rqy	.ch3	
.scd	.wk?	.pre	
.wri	.wq1	.ppa	
.wpd	.slk		

Table 6.2 Settings and System Components Migrated by Default by USMT

Settings and System Components Migrated	
Accessibility options	Microsoft® Outlook® settings and store
Classic Desktop settings	Microsoft® Outlook® Express settings and store
Dial-up connections	Phone and modem options
Display properties	Regional options
Folder options	Screen saver selection (not users' personal screen saver files)
Fonts	Shortcuts (shell tools, network items, and so forth)
Microsoft® Internet Explorer settings	Sounds and audio devices settings
Localization/International settings	User certificates (personal, e-mail, Microsoft® Internet Explorer security, and so forth)
Microsoft® Office settings	Taskbar settings
Mouse and keyboard settings	
Network drives and printers	

USMT offers multiple customization options for including various file types and settings in the user state migration. Administrators should expect to customize the default set of data and settings. Customization should be performed by technical personnel with knowledge of the registry.

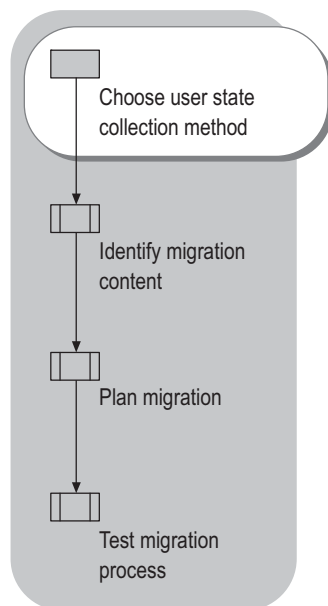
This chapter describes how to plan and test a user state migration, but does not describe how to use the USMT tool. For code samples to assist you in customizing the .inf files used with USMT and the Files and Settings Transfer Wizard, see the file Inf Commands.doc included on the Windows Server 2003 operating system CD in the folder \ValueAdd\Msft\USMT. For more information about using USMT, see the User State Migration Tool Reference Materials link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources/>.

Choosing a User State Collection Method

The first step in planning your user state migration is to determine the best way to collect user state in your environment (Figure 6.2). Four user state migration methods are available for collecting and restoring user state:

- Manual migration
- Scripted-manual migration
- Centralized automation
- User-driven migration

Figure 6.2 Choosing a User State Collection Method



The method by which you deploy Windows XP affects which user state migration method you should choose. Table 6.3 explains how each system deployment method affects the environment into which the user state will be migrated. A clean environment reduces management and support requirements.

Table 6.3 Effects of Windows XP Deployment Methods on User State Migration

Deployment Method	Effects on User State Migration
Wipe-and-load. The computer's hard drive is reformatted before installing Windows XP. This is the recommended deployment method when the existing hardware is sufficient to run Windows XP, because it provides a clean platform on which to restore applications and settings.	Presents a completely clean environment in which to restore user state.
Parallel deployment. The original computer is replaced with a new computer running Windows XP. This is the recommended deployment strategy when the old computer has insufficient hardware capability to run Windows XP. You can keep the original computer running until you are sure that the new computer is completely functional.	Presents a completely clean environment in which to restore user state. Commonly used when deployment of Windows XP is timed with computer replacement, as in lease rollover.
Operating system upgrade. The original computer is upgraded using the Upgrade option during the setup phase of Windows XP deployment. This leaves the user's files, folders, settings, and installed applications intact.	Does not provide a clean environment, thereby increasing support and management costs. The migration of System Policy, registry settings, files, drivers, DLLs, and folder hierarchies can cause problems and nonstandard installations. Not recommended in production environments.

When determining the best user state collection method for your situation, weigh these factors:

- The size of your organization
- The number of users to be migrated
- The level of desktop management already in place
- The uniformity of file locations on workstations
- The type of technical personnel available to assist in the migration
- The amount of time you can dedicate to the migration process

Each migration method is particularly well suited to specific scenarios. It is likely that a large corporate deployment will involve several of these scenarios and employ a mixture of migration methods.

Manual Migration

In a manual migration, an onsite technician personally attends each computer, typically performing these tasks:

- Ensures that the user's computer is ready for migration (for example, checks to see whether all important files are in the folders that are being migrated).
- Collects the user state by running either USMT (the Scanstate.exe command-line tool) or the Files and Settings Transfer wizard.
- Deploys Windows XP either by providing a new computer running Windows XP or by doing a wipe-and-load deployment of Windows XP. (Remote Installation Services [RIS] provides a convenient way to deploy a common Windows XP image.)
- Restores the user state by again running either USMT (the Loadstate.exe command-line tool) or Files and Settings Transfer wizard. The same tool that is used to collect user state must be used to restore it.
- Is available to help with any issues while the user checks to make sure that everything has been migrated properly.

Because technical labor costs in manually collecting state data can be very high, it is often beneficial to combine manual collection with the use of automated scripts.

Table 6.4 summarizes advantages and disadvantages of manually migrating user state. Because of the noted disadvantages, a strictly manual approach is not recommended.

Table 6.4 Advantages and Disadvantages of Manual User State Migration

Advantages	Disadvantages
<ul style="list-style-type: none"> • A technician is available to deal with unexpected problems. • Users are reassured by having a person to ask questions of during the migration. 	<ul style="list-style-type: none"> • Expensive because of high technical labor costs. • Slow because a technician must visit each computer individually. • Higher chance of human error than with automated methods. • Does not scale to distributed or remote office scenarios.

Scripted-Manual Migration

By supplementing a manual deployment with scripting, you can reduce the costs of an exclusively manual approach while providing the flexibility to handle special situations.

Scripting speeds up the process of migrating user state on individual computers, enabling a technician to migrate user state on multiple computers in the same physical area simultaneously. This greatly reduces the likelihood of human error, yet maintains the advantage of having someone onsite to deal with unexpected problems. During scripted-manual migrations, you also can use less skilled technicians for the onsite phase of the migration.

Table 6.5 summarizes the advantages and disadvantages of using a scripted-manual approach for migrating user state. Scripted-manual migration is the recommended approach for a parallel deployment.

Table 6.5 Advantages and Disadvantages of Scripted-Manual User State Migration

Advantages	Disadvantages
<ul style="list-style-type: none"> • A technician is available to deal with unexpected problems. • Users are reassured by having a person to ask questions of during the migration. • Lower chance of human error than with a purely manual migration method. 	<ul style="list-style-type: none"> • Requires that a technician be onsite, with physical access to each computer that is being migrated. • Requires that script files be created. • Does not scale to distributed or remote office scenarios.

The manual-scripted migration process for a wipe-and-load deployment, in which the computer's hard drive is reformatted before the new operating system is installed, is slightly different from the process for a parallel deployment.

Migration Process in a Wipe-and-Load Deployment

In a wipe-and-load Windows XP deployment, use this combination of scripted and manual steps:

1. Create scripts to collect and restore user state.
2. Have a technician perform the following tasks at each computer:
 - a. Run the script for collecting user state.
 - b. Format the computer's hard drive and run RIS to install the new operating system image.
 - c. Log on as the administrator, and run the restoration script.
3. Have the computer's user log on and check for proper restoration of data and settings.

Migration Process in a Parallel Deployment

Perform these steps to migrate user state in a parallel deployment:

1. Create two scripts for each computer that is to be replaced, one for collecting user state and the other for restoring user state.
2. On the computer that will be replaced, run the script for collecting user state.
3. On the new computer:
 - a. Install Windows XP.
 - b. Log on as the administrator, and run the script for restoring user state.
4. Have the computer's user log on to the new computer and check for proper restoration of data and settings.

Centralized Automation

With centralized automation, you can extend the efficiencies available through the scripted-manual method for migrating user state. To centralize automation of user state migration, you refine the user state collection and restoration scripts to such a degree that no onsite input from a technician is required. IT technicians can deploy the scripts to targeted computers from a remote location.

Centralized automation enables enormous cost savings and provides a common migration experience corporation-wide. Centralized automation does not work well in parallel deployments because of the complexity in determining target and destination computer addresses for a large number of computers, but it is ideal for wipe-and-load deployments.

Table 6.6 summarizes the advantages and disadvantages of using centralized automation to migrate user state. Centralized automation is the ideal solution for wipe-and-load deployments.

Table 6.6 Advantages and Disadvantages of Centrally Automating User State Migration

Advantages	Disadvantages
<ul style="list-style-type: none"> Allows simultaneous migration of user state for large numbers of computers (limited only by network bandwidth and server storage). Produces results that can be replicated. Produces a common user experience. Scales well to distributed or remote office scenarios. 	<ul style="list-style-type: none"> Requires that script files be created. Does not work well in parallel deployments.

The key challenges in the centralized automation of user state migration are:

- Targeting and deploying scripts so that they run on the user's computer in the appropriate context.
- Associating user state with a specific computer.
- Creating scripts that create a temporary store for each user's state and then access that store to restore the state on the destination computer.
- Automatically deploying the Windows XP image with no one attending the remote computer to accept the RIS image.

Targeting and deploying scripts to run in the appropriate context

Follow these rules when targeting and deploying automated scripts during user state migration:

- The collection script must run under the user's logon account.
- The restoration script must run securely in the administrator's context with no one attending to the remote computer to log on.
- The computer's user should not be using the computer when the script is run.
- No applications can be running when the script is run.

Several options are available for automatically running the script at a specific time and under in the appropriate context. It is best to use a management solution such as Microsoft® Systems Management Server (SMS) for this. SMS provides advanced targeting options, contains software deployment structural components, and can target packages to run at specific times in specific contexts. Other options include logoff scripts, e-mail that includes the script (which automatically shuts down the mail client), or deployment automation delivered by way of a Web site.

For more information about Systems Management Server, see the SMS Product Information link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Associating user state with a computer When deploying a standard image to a series of computers, plan how to discover which user's state to restore to which computer. Two common methods for identifying computers are by the media access control (MAC) address for the network adapter or by the serial number of the processor.

For example, you can write a script that collects both the network adapter MAC address of the computer and the logon name of the user. This data pair is stored in a central database along with the mapping of the user state storage location. When restoring user state, the script looks up the network adapter MAC address to find the user's logon name and user state storage location, and restores the user state to the appropriate computer.

Storing and restoring the user state In centralized automation, you can use the same scripts that collect and restore user state in the scripted-manual method, with these adjustments:

- The collection script must be able to create a separate subdirectory for storing each user's state during the migration. Appending the user's logon name to the root storage path (for example, `\\State\Username`) is a good solution. If the user has multiple computers, use both the computer name and the user's logon name (for example, `\\State\Username\Computername`).
- The restoration script must read the user state storage path from the central database that the collection script wrote to and restore the user state from the appropriate storage location.

Automating Windows XP image installation Microsoft offers several options for deploying operating systems. For information about your options for automating the deployment of a Windows XP image, see "Choosing Your Automated Installation Method" in *Automating and Customizing Installations* of this kit.

User-Driven Migration

Perform a user-driven user state migration when no central management is in place for a deployment, or when users connect to the organization's network from a remote location.

In a user-driven migration, have the user run the Files and Settings Transfer Wizard to collect and restore user state. The user can use the same customized .inf files that you might use with USMT in other types of migrations. With the Files and Settings Transfer Wizard, the user can decide which applications and components to migrate (although you set the defaults), and can add and remove files and folders from the set to be migrated. Be prepared to offer these users some training on using the wizard and the .inf files.

Table 6.7 summarizes the advantages and disadvantages of a user-driven migration of user state. User-driven migration is the recommended approach for nonmanaged environments and remote users.

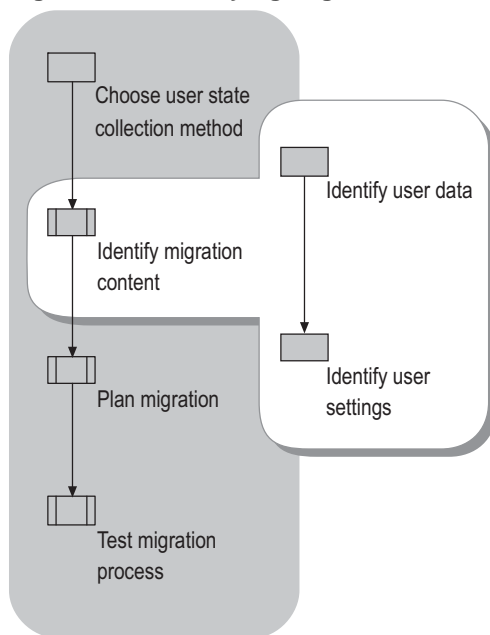
Table 6.7 Advantages and Disadvantages of User-Driven User State Migration

Advantages	Disadvantages
<ul style="list-style-type: none"> • Controlled tool better enables users to drive their own migration. • Can use the data captured using customized .inf files. 	<ul style="list-style-type: none"> • IT staff are not involved in the actual migration; relies on the user's judgment. • No standard storage location. • Minimal control over what is migrated, resulting in a less standardized desktop.

Identifying Migration Content

After determining how to perform the migration, identify which user files and folders to migrate, and then identify key user settings to migrate, as shown in Figure 6.3. Consider which data and settings are worth migrating and which do not provide sufficient benefits to justify the cost of migration.

Figure 6.3 Identifying Migration Content



Part of identifying migration content is recognizing that you must provide a transitional storage place for everything that you migrate. Be sure that you have enough room to store the aggregate content during the migration. For information about estimating required storage capacity, see “Determining Storage Requirements” later in this chapter.

Identifying User Data to Migrate

When identifying what data to migrate, consider these questions:

- Do users save their files in a single folder or in files scattered across a hard disk?
- Which data files do the users work with regularly?

One way to determine which user data to migrate is to identify folders to migrate based on known locations. These can be locations that the system is aware of, such as the My Documents folder and Favorites, or locations that the organization-specifies, such as `\EngineeringDrafts` or `C:\Data`.

Another way is to identify the applications that the users use and then look for files with corresponding file types. Organizations commonly use an e-mail package and productivity suite such as Microsoft Office. These applications typically use specified file name extensions. For example, Microsoft® Word primarily uses the .doc file name extension. However, Word also uses file types such as templates (.dot files) and hypertext files (.htm files).

If you use this method to identify files to migration, create a list of important file types based on applications that your organization uses. A good starting point for identifying the file types to migrate is to look at the registered file types on the standardized desktop image that you will install. The registered file types are listed in **Folder Options**.

► **To view a list of registered file types**

1. Double-click the My Computer icon on the desktop.
2. On the Tools menu, click Folder Options.
3. Click the File Types tab to display the registered file types.



Important

Do not attempt to migrate the applications associated with the files. Instead, reinstall the applications from a software distribution point, or include them in the standard desktop image.

Identifying User Settings to Migrate

Consider the following questions when identifying which user settings to migrate:

- Are you moving toward a more managed environment? If so, which settings will users be able to change in this new environment?
- Which settings do the users need to get their work done?
- Which settings make the work environment comfortable for users, allowing them to be more productive?
- Which settings will reduce support desk calls after the migration?

Identifying Key Settings for User Productivity

List the important settings that the user needs to become productive immediately after the migration. These settings might include an e-mail server and account, a remote access connection, an Internet connection, and accessibility features. One good place to find the relevant settings is in your organization's system configuration handbook for new users.

Locating application-specific settings can be time-consuming, because various applications store settings in different locations. Therefore, limit your list to settings that the user must have to maintain productivity.

Some applications provide tools that scan the registry and then display settings and their storage location in a format that is easy to read. For other applications, you must compare registry entries before and after an installation to trace the settings.

Typically, the user settings for an application are stored in the registry in the subkey `HKEY_CURRENT_USER\SOFTWARE\Companyname\Application`. To compare before and after images of the registry in order to find the updated entries, you can use the Sysdiff.exe tool, documented and available for download from the Resource Kit Tools link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources/>.



Caution

Do not edit the registry unless you have no alternative. The registry editor bypasses standard safeguards, allowing settings that can damage your system, or even require you to reinstall Windows. If you must edit the registry, back it up first and see the Registry Reference on the *Microsoft® Windows® Server 2003 Deployment Kit* companion CD or at <http://www.microsoft.com/reskit>.

Evaluating Costs vs. Benefits of Migrating Settings

It is not always cost-effective to collect and restore all user-specific settings in the registry. In deciding which settings to migrate, weigh the cost of lost productivity while users recreate their settings against the IT costs of migrating them.

To determine the cost-effectiveness of collecting settings:

1. Perform the following calculations:
 - a. Determine the number of users whose user state will be migrated.
 - b. Multiply that number by the average time that it takes a user to reconfigure his or her settings.
 - c. Multiply the result by the users' average hourly wage.
2. Compare this cost with the costs involved in tracing, collecting, and restoring the settings.

Table 6.8 shows user cost calculations for an enterprise with 5,000 users who have an average hourly wage of \$20, based on an estimated reconfiguration time of 2 hours per user. The total user costs for not migrating user settings are compared with estimated IT costs for migrating the settings, shown in the final column.

Table 6.8 Sample Cost Comparison for Migrating vs. Not Migrating User Settings

Number of Users	User Reconfiguration Time	Average Hourly Wage	Total User Costs (No Migration)	Estimated IT Costs for Migration
5,000	2 hours	\$20.00	\$200,000.00	\$50,000

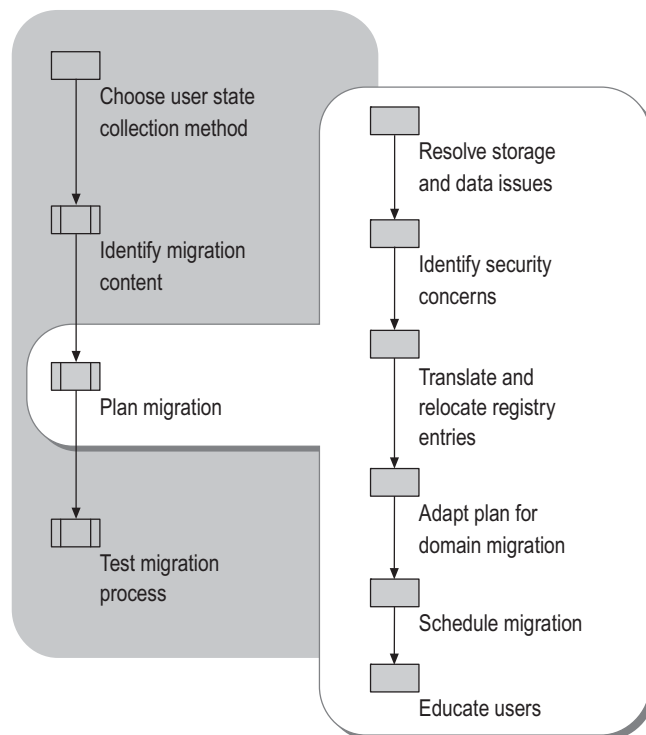
Less measurable, but equally important, is the time that IT professionals and the Help desk staff spend in helping users to reconfigure desktops when their personal settings are not migrated.

Not migrating settings also can lead to lost productivity and decreased morale. Familiar desktop settings help users learn about the new system more easily, and reduce the potential for help desk calls. While the value of migrating some personal settings might not be immediately apparent, it is worthwhile to capture the settings that make new computers familiar and comfortable to users — for example, desktop settings, display settings, and folder options. If such settings are not migrated, productivity decreases while users adjust these settings to the way that they prefer them.

Creating a Detailed Migration Plan

After selecting a collection method and identifying the content to migrate, review the technical details involved in a successful migration and devise a detailed migration plan that addresses storage and security issues, resolves changes in registry settings from earlier versions of Windows, and includes adjustments for concurrent domain migration if applicable. Include a migration schedule and detailed instructions for users in your migration plan. Figure 6.4 shows the tasks involved in creating a detailed plan for user state migration.

Figure 6.4 Creating a Detailed Migration Plan



Resolving Storage and Data Issues

Because the process of migrating user state consists of moving data, the first step in preparing for your migration is to identify and resolve storage and data concerns associated with the move. Determine how much intermediate storage space is required for the data that is being moved. Verify that your selection of user data and settings to be migrated is complete as well as cost-effective. Plan how to resolve any file name conflicts or other file relocation issues that might arise during the migration.

Determining Storage Requirements

Determine how much disk space is required for an intermediate storage location for user state. Base your calculations on the volume of e-mail, personal documents, and system settings for each user. The best way to estimate these is to survey a few average desktops to estimate the size of average stores in your environment.



Important

Allow a minimum buffer of 20 percent additional space in the intermediate storage location. To enhance performance, locate the intermediate store on high-speed drives. Ensure that the intermediate storage of user state is the only task that the store performs and that it has an optimized (high-speed) network connection.

Email If users deal with a large volume of e-mail or keep e-mail on their local computers instead of on a mail server, the e-mail can take up as much disk space as all other user files combined. (This is not a factor if the e-mail is stored on a server only.) Prior to migrating user data, make sure that users who store e-mail locally synchronize with their mail server.

User documents The types of documents that an organization uses can make a substantial difference in storage requirements. For example, an architectural firm that predominantly uses Computer-Aided Design (CAD) files needs much more space than does a law firm dealing primarily with word processing documents. If your users already store many documents on file servers through such mechanisms as Folder Redirection, and they will have access to these locations after the migration, you do not need to migrate those documents.

User system settings Typically, 5 MB of storage is adequate to save a user's registry settings. This requirement can fluctuate based on the number of applications installed over the lifetime of the computer, but it is rare for the user-specific portion of the registry to exceed 5 MB.

Reviewing Data Collection and Restoration Selections

If you are using the User State Migration Tool (USMT), in most cases you will customize the .inf files included with the tool to limit the operating system and application settings that are migrated and to include additional file types and folders.

When customizing the .inf files, it is important to keep a backup copy of the original files and to thoroughly test your customizations. To yield the best results, keep the rules in the .inf file as simple as possible.

For information about the default files and settings that USMT migrates, see “User State Migration Tools” earlier in this chapter. For more information about using USMT, see the User State Migration Tool link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources/>.

Addressing File Relocation Issues

If you change the computer hard disk configuration during migration, you might not be able to restore files to the same drive or directory structure from which they were collected. For example, if you replace two small drives with one large drive, the second drive will not be available to receive the collected user data. In this case, you must relocate the files.

A relocated file might be written to a folder that already contains a file with the same name, causing a name conflict. USMT handles this problem by appending “(1)” to the original filename, and incrementing that number for each new file with the same name. For example, if two files by the name of Example.doc were written to a directory that already contained an Example.doc file, the relocated files would be named Example(1).doc and Example(2).doc.

One way to avoid file name collisions when you move files is to duplicate as much of the original path as possible in the new location. For example, if the full path and file name of the original file was D:\EngineeringDrafts\Example.doc, and the new root location is C:\Documents and Settings\Username\My Documents, create the new path and file name C:\Documents and Settings\Username\My Documents\EngineeringDrafts\Example.doc.

Identifying Security Concerns

Maintaining security during and after user state migration is a significant issue. In particular, take into consideration these issues:

- Typically, the Access Control Lists (ACLs) associated with files and folders are not migrated, so the ACLs must be restored or recreated.
- Encrypting File System (EFS) information is not migrated, and encryption that occurs during migration affects who can read the files in their new destinations.
- In some organizations, it is deemed critical to secure user state during a migration.

Restoring Lost Access Control Lists (ACLs)

In planning user state migration, it is best to assume that access control lists will not migrate during your user state migration. Several factors affect the migration of ACLs:

- The USMT tool and the Files and Settings Transfer Wizard do not migrate ACLs — instead, default ACLs are assigned to each folder that is created on the destination computer.
- If users are changing domains during a migration, there is a good chance that the original ACLs will not work unless you use a tool such as SIDHistory as part of the user state migration process. For information about managing access control lists during a domain migration, see “Designing the Active Directory Logical Structure” in *Designing and Deploying Directory and Security Services* of this kit.
- When you migrate a Windows NT workstation that uses an NTFS file system drive, ACLs for individual files often do not migrate with the files. Instead, the files inherit the default ACLs of the folder into which they are copied.

Managing Data Encryption During Migration

Encrypting File System (EFS) certificate data is not migrated when you use either USMT or the Files and Settings Transfer Wizard. The two tools treat encryption differently during a user state migration:

- The Files and Settings Transfer Wizard decrypts encrypted files during migration, and does not encrypt the files when it writes them to the destination computer (unless writing them to a folder that is encrypted).
- USMT decrypts encrypted files during migration, but if the temporary store is encrypted, the file will be encrypted under the user’s credentials (since Scanstate.exe is run in the user’s context). In addition, if the destination folder for the migrated file is encrypted, the restored file might be encrypted and, because the file will have been written under the administrator’s credentials, the administrator, not the user, will be able to read the file.

In general, assume that files are not protected by encryption during a user state migration. Furthermore, because EFS certificates are not migrated, if a file does get encrypted during the migration, the user will not be able to read the file unless the EFS certificate is recovered from the network. For information about performing this type of operation, see “Encrypting File System” in *Microsoft® Windows® XP Professional Resource Kit Documentation* (or see “Encrypting File System” on the Web at <http://www.microsoft.com/reskit>).

Securing User State During Migration

In some organizations, keeping the user's state secure from the IT technician who is performing the migration is a potential issue. In general, of course, IT technicians should be trusted people.

If the IT technician's access to user state is a security concern for you, take these steps:

- Have the user drive the migration using either USMT or a scripted-manual method. Under the scripted-manual method, the user must be able to restore user state by logging on as the administrator.
- When securing the state in the temporary store, make sure that while the root folder might allow full user access, the individual user folders only allow access for IT staff and the owner of the folder.
- To protect data as it traverses the network, use Internet Protocol security (IPSec) or other network security protocols to secure these transfers.

Translating and Relocating Registry Entries

Because the name or location of some registry entries for the operating system has been changed in later versions of Windows, many registry values must be translated during migration, and others must be relocated within the registry. This is also true with different versions of some applications. For example, copying the subkey `HKEY_CURRENT_USER\Control Panel\Desktop\WindowsMetrics` during migration causes problems, because entries such as **IconFont** are not translated correctly.

USMT automatically translates and relocates the operating system settings for the user state that it migrates. To prevent problems with custom settings, either do not migrate entries that are unique to a specific version of an application and cause problems, or use the renaming and relocating capabilities of USMT to adjust the entries. You cannot use USMT to translate registry values: The best solution for this type of change is to write custom code.

You can use tools such as Sysdiff.exe to compare before and after images of the registry. This tool helps in finding registry changes between versions of an application or between the same version of the application running on different versions of Windows. Sysdiff.exe is documented and available for download from the Resource Kit Tools link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources/>.

Windows XP registry restrictions

The enhanced security of Windows XP can mean that registry settings that were accessible in the Microsoft® Windows® 95 or Microsoft® Windows® 98 operating systems are no longer accessible.

In Windows XP, a user with no administrative permissions has write access to only three locations (depending on default security settings): the HKEY_CURRENT_USER registry subtree, the User Profile, and a shared documents location. Users cannot change settings outside those locations without administrative permissions.

If an application writes settings outside HKEY_CURRENT_USER, users will not be able to run the application after migration. You should deal with these applications on a case-by-case basis. Sometimes it is acceptable to change the access rights to a part of the registry; at other times, this can grant to the user unacceptable access to the registry. The best solution is to work with the software vendor or in-house developer to determine migration requirements when introducing a revised version of an application.

Adapting Your Plan for Domain Migration

Domain migration introduces additional issues for user state migration. Command-line parameters available in USMT make it easy to change the domain name and the user name during a migration. However, these switches do not resolve issues related to security identifiers (SIDs) during domain migration.

The Active Directory Migration Tool (ADMT) addresses issues that USMT does not handle. This tool can help you to diagnose possible problems before starting migration operations.

ADMT provides the following capabilities:

- Using task-based wizards, you can migrate users, groups, and computers; set correct file permissions; and migrate mailboxes for Microsoft® Exchange Server.
- Using the tool's Reporting feature, you can assess the impact of the migration both before and after move operations.
- The tool also provides support for parallel domains, so that you can maintain your existing domains under the Microsoft® Windows NT® version 4.0 operating system while you deploy a later version of the Windows operating system (Microsoft® Windows® 2000; Windows® Server 2003, Standard Edition; Windows® Server 2003, Enterprise Edition; or Windows® Server 2003, Datacenter Edition).

For information about issues related to the migration of domain user objects and how domain migration affects the migration of user state, see the ADMT Cookbook link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Scheduling Your Migration

Consider the impact of the migration on network bandwidth. The user state traverses the network as it is being moved to a temporary storage location on a network server and again when moved to the destination computer.

To minimize the impact of your migration on users and your network, follow these general guidelines:

- Minimize the impact on the network while other people need to use it by scheduling migrations during off-peak hours.
- Trying to move too many users at a time risks network collisions. Determine the optimal number of users to migrate at a time.
- Minimize the use of network capacity by locating storage servers close to the clients (for example, on the same subnet).
- Keep in mind the simple impact of migration on your normal flow of business. Work with the teams that you are migrating to ensure that the migration will not jeopardize any crucial projects. Determine whether teams need to be migrated as a group.

Educating Users

To minimize productivity loss and support costs, prior to migration, set user expectations to match the results that you obtained during pilot testing. Set expectations early and clearly to reduce user frustration and Help desk calls.

Provide a schedule that indicates when each user's computer will be migrated, as well as clear guidelines that tell exactly what the user needs to do to prepare for the migration. Your migration plan must include backing up user files, verifying that applications that use synchronization mechanisms (such as e-mail) are also backed up, and preparing for changes to the desktop.

Preparing files and folders for migration The period just before migration is a good time for users to get their files into a stable state. For example, if version control software is in use, make sure that all users check in all files that they have checked out. If users are supposed to save all in-progress documents in a specific network folder, make sure that the users save all relevant files to that folder.

If the user state collection process will retrieve data only within a known folder (for example, My Documents), have users move all of their important documents to that folder. If the folder that contains all of these files is a network share, no migration of the files is needed as long as the user has access to that share from the new system.

Preparing e-mail and other applications that must be synchronized

It is recommended that users send all pending e-mail prior to migration. Along with e-mail, My Briefcase, Microsoft Outlook, Microsoft® Notes, and any other application or feature that uses synchronization must be synchronized prior to the migration.

Preparing users for changes to the desktop The more closely that the users' new environment mirrors their previous one, the less support they will need, and the sooner they can resume productivity. If the migration involves changes to the desktop, prepare the users for these changes.

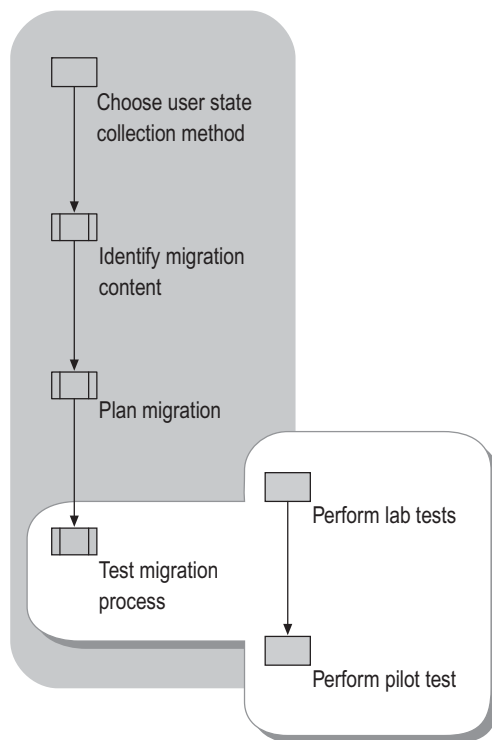
If you will not migrate specific settings, tell users in advance which settings they will need to reenter and which related files they might need to migrate (for example, a personal photograph used as a background on the user's desktop).

If you will migrate your users to the new Windows XP Luna desktop, let them know to expect the change. If you are using USMT, you can optionally migrate their "classic desktop" if you need to delay this change until the users have had training in how to use the new Luna desktop.

Testing Your Migration Process

Before rolling the migration out to a large number of computers, test the process in a controlled laboratory setting, and then run a pilot test. Figure 6.5 shows the tasks in the testing process.

Figure 6.5 Testing Your Migration Process



Even with thorough testing before the migration, you often can improve the process by making adjustments as the migration proceeds. It is best to move groups of users in phases. Migrate one group or team and make sure the migration is successful before starting the next group. This gives you a chance to modify your plan as needed between groups.

Performing Lab Tests

In the lab test, match your test environment closely to your production network:

- Use the same type of server in your test environment as in your real environment. If you will migrate users from an old domain to a new domain, include both the old and new types of servers in your test environment.
- Run a test migration from at least one computer running each operating system from which you will migrate. For example, if you need to migrate user state from some computers running Microsoft® Windows® 98, some running the Microsoft® Windows NT® Workstation version 4.0 operating system, and some running the Microsoft® Windows® 2000 Professional operating system, test at least one computer running each operating system.
- Make backups of the data residing on the computers from which you are migrating user state so that you can easily reproduce any problems that you encounter. If you adjust a custom script to solve a problem, it is hard to know whether the change solved the problem if you cannot reproduce the problem.

Performing a Pilot Test

After thoroughly testing your user state collection, operating system deployment, and user state restoration processes, conduct a pilot test on a small group of users in a production environment.

In the pilot test, concentrate on these areas:

- Make sure that all data and settings migrate as expected.
- Note the storage space requirements for the pilot data and adjust your initial calculations accordingly.
- If unexpected problems arise, address them before going further.

As you did during lab testing, make backups of the data on your source computers so that, for testing purposes, you can easily reproduce any problems that you encounter.

Only after you are fully satisfied with the success of your pilot test should you begin a full migration.

Additional Resources

These resources contain additional information related to user state migration for Windows XP.

Related Information

- “Designing RIS Installations” in *Automating and Customizing Installations* of this kit for information about using Remote Installation Services (RIS).
- The Windows Deployment and Resource Kits Web site at <http://www.microsoft.com/reskit> for information about scripting in a Windows Server 2003 environment.
- The MSDN Scripting Clinic link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources> for information about scripting in a Windows Server 2003 environment.
- The file `Inf Commands.doc`, included on the Windows Server 2003 operating system CD in the folder `\ValueAdd\Msft\USMT`.

Related Tools

- User State Migration Tool (USMT)

This command-line tool is used to collect a user's documents and settings before an operating system migration to Windows XP from an earlier version of Windows and to restore them after the installation. For a reference to the commands and syntax employed in the `.inf` files that are used to customize the selection of files, settings, and registry entries migrated by USMT, see the User State Migration Tool Reference Materials link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

- Files and Settings Transfer Wizard

The Files and Settings Transfer Wizard enables users to migrate personal display properties, folder and taskbar options, and Internet browser and mail settings, as well as specific files or entire folders, such as My Documents, My Pictures, and Favorites, without manual configuration. For more information about the Files and Settings Transfer Wizard, see Help and Support Center for Windows XP.

- Sysdiff.exe

Sysdiff.exe is an automated installation tool that enables you to pre-install applications, including applications that do not support scripted installation, as part of an automated setup. For more information about Sysdiff.exe, see the Sysdiff.exe link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

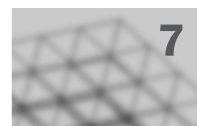
- Windows 2000 Active Directory Migration Tool (ADMT)

The Active Directory Migration Tool (ADMT) is used to migrate to the Windows 2000 Active Directory® directory service, providing a task-based wizard that is used to migrate users, groups, and computers; to set correct file permissions; and to migrate Microsoft Exchange Server mailboxes. For information about ADMT, see the Active Directory Migration Tool (Windows 2000) link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Related Job Aids

- “Worksheet A.34 Identifying Data and Settings for Migration” (DMEUSE_34.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.34 Identifying Data and Settings for Migration” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.35 Evaluating Costs vs. Benefits of Migrating Settings” (DMEUSE_35.doc) on the *Microsoft® Windows® Server 2003 Deployment Kit* companion CD (or see “Worksheet A.35 Evaluating Costs vs. Benefits of Migrating Settings” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.36 Choosing an Intermediate Data Store” (DMEUSE_36.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.36 Choosing an Intermediate Data Store” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.37 Collecting User State Information” (DMEUSE_37.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.37 Collecting User State Information” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.38 Preparing for the Migration” (DMEUSE_38.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.38 Preparing for the Migration” on the Web at <http://www.microsoft.com/reskit>).

Implementing User State Management



By implementing the user data management and user settings management features that IntelliMirror® management technologies offer, you can centrally manage and control desktops, settings, and user data for large or small groups throughout your organization. Users can also move from one workstation to another and still have access to their own data, settings, and familiar desktop.

In This Chapter

Implementing User State Management Overview

Planning for User State Management

Designing Configurations for Managed Desktops

Preparing for Deployment

Configuring User State Management Features

Additional Resources

Related Information

- For more information about managing and reconfiguring desktops, managing user data and settings, and the infrastructure and mechanics of Group Policy, see the *Distributed Services Guide* of the *Microsoft® Windows® Server 2003 Resource Kit* (or see the *Distributed Services Guide* on the Web at <http://www.microsoft.com/reskit>).
- For more information about implementing Group Policy, see “Designing a Group Policy Infrastructure” in this book.

Implementing User State Management Overview

To ensure that users’ data, applications, and settings remain constant throughout the users’ environments, you can use IntelliMirror technologies on the server and the clients. Active Directory® directory service and Group Policy provide the foundation for IntelliMirror. Using

Group Policy to define managed desktop configurations enables IntelliMirror to deploy, recover, restore, and replace users' data, software, and personal settings.

By deploying IntelliMirror technologies to manage users' data and settings, you provide the following advantages:

- Users' data is protected, up to date, and highly accessible. Users can access their data from any computer on the network. To enable these capabilities, you can redirect specific user data folders, such as the My Documents folder, to a network location, and then make this location available to users for offline use.
- Users' preferences and settings for the desktop and applications are available wherever the users log on. By creating a preconfigured, customized desktop, based on the users' jobs, you can provide a consistent desktop environment and system settings, and you can reduce support calls and minimize the time and cost that is associated with replacing computers.
- You can also centrally manage software installations, updates, repairs, upgrades, and software removal by performing a Group Policy–based software installation.

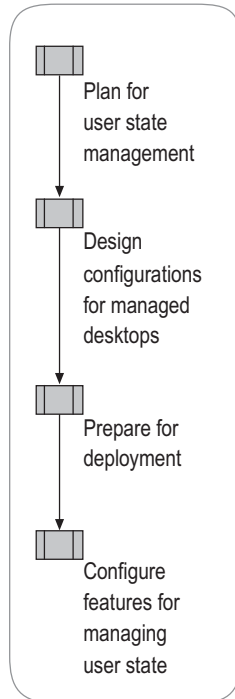
You start your deployment plan by defining your objectives for managing user data and settings, and then you assess the needs and resources of your organization. You can then determine which IntelliMirror technologies meet the needs of your users and your organization. After you design the managed desktop configurations for the various types of users and computers in your organization based on their requirements, you must test your designs in a controlled environment and instruct your users about the technologies that you are deploying.

User State Management Implementation Process

The process of implementing user state management typically entails four phases. Begin by developing a plan for managing user data and settings. Before beginning your design, you must fully understand your organization in terms of the users' requirements, computer roles, the current network environment, your organization's security requirements, and corporate policies. Then design your managed desktop configurations based on the requirements of the various types of users and computers in your organization. The next phase consists of thoroughly testing the configurations before you deploy them and preparing your users by informing them about the technologies you will use to configure and manage their data and settings.

Figure 7.1 illustrates how to structure your approach to implementing user state management.

Figure 7.1 Process for Implementing User State Management



Technology Background

Many users must work with network-based files, even when their computers are not connected to the network. IntelliMirror technologies, such as Folder Redirection and Offline Files, make data and settings available to users even when the network is not. This increased availability is a result of storing user data and settings on network servers, while maintaining local copies of selected files and folders.

The IntelliMirror management technologies that are included in Microsoft® Windows® 2000, Microsoft® Windows® XP, and Microsoft® Windows® Server 2003, Standard Edition; Windows® Server 2003, Enterprise Edition; and Windows® Server 2003, Datacenter Edition, operating systems provide directory-based change and configuration management capabilities. By using IntelliMirror technologies on the server and the client, a user's data, applications, and settings remain consistent throughout the user's environment. When you use Windows XP and Windows 2000 clients, and Windows 2000 Server, and Windows Server 2003 networks with Active Directory, you can take full advantage of IntelliMirror and Group Policy management features. Active Directory and Group Policy provide the foundation for IntelliMirror. Based on the Group Policy settings you specify, IntelliMirror can deploy, recover, restore, and replace a user's data, software, and personal settings.

For more information about Group Policy, see the *Distributed Services Guide* of the *Windows Server 2003 Resource Kit* (or see the Distributed Services Guide on the Web at <http://www.microsoft.com/reskit>). For more information about Active Directory, see the

Directory Services Guide of the *Windows Server 2003 Resource Kit* (or see the *Directory Services Guide* on the Web at <http://www.microsoft.com/reskit>).

Table 7.1 describes the advantages of using the core technologies in IntelliMirror that support user state management.

Table 7.1 IntelliMirror Features and Technologies for User State Management

IntelliMirror Feature	Advantages	Technologies
User data management	Data is protected and highly available. Users can access their data from any computer on the network.	Active Directory Group Policy Offline Files Folder Redirection Synchronization Manager Disk Quotas Enhancements to the Windows shell
User settings management	Users get their preferred desktop configuration from any computer on the network. User preferences and settings for the desktop and applications are available wherever the user logs on.	Active Directory Group Policy Offline Files Roaming User Profiles Enhancements to the Windows shell
Computer settings management	Administrators can use Group Policy to define the appearance and behavior of the desktop. For example, you can set options for the programs that appear on the desktop and options for the Start menu.	Active Directory Users and Computers snap-in Group Policy
Software installation and maintenance	Administrators can centrally manage software installations, updates, repairs, and removal.	Active Directory Group Policy Software Installation (an extension of Group Policy Object Editor) Windows Installer

Active Directory

Windows-based directory service, Active Directory, stores information about objects on a network and makes this information available to administrators and users. By using Active Directory, you can view and manage network objects on the network from a single location, and users can access permitted network resources by using a single logon. Active Directory Users and Computers Microsoft Management Console (MMC) snap-in is the recommended tool for managing Active Directory objects, including organizational units (OUs), users, contacts, groups, computers, printers, and shared-file objects.

To manage sites and services, use the Active Directory Sites and Services MMC snap-in. To administer domains and trusts, use the Active Directory Domains and Trusts snap-in.

Group Policy

The infrastructure within Active Directory that enables directory-based configuration management of user and computer settings on computers running Windows® Server 2003, the Windows® 2000 family, and the Microsoft® Windows XP Professional operating systems. By using Group Policy, you can define configurations for groups of users and computers, including policy settings for Windows Server 2003 registry-based policies, software installation, scripts, folder redirection, Remote Installation Services, Microsoft® Internet Explorer maintenance, and security.

The Group Policy settings that you create are contained in a Group Policy object (GPO). To create a GPO, use the Group Policy Management Console MMC snap-in (GPMC). To edit policy settings in GPOs, use the Group Policy Object Editor, which can be started from the GPMC. By using GPMC to link a GPO to selected Active Directory system containers — sites, domains, and OUs — you apply the policy settings in the GPO to the users and computers in those Active Directory containers.

For more information about Group Policy and GPMC, see “Designing a Group Policy Infrastructure” in this book. To download GPMC from the Microsoft Download Center; see the Group Policy Management Console link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

User Data and User Settings

Before you deploy IntelliMirror technologies, it is useful to understand the distinctions between user data and user settings. *User data* describes the files that a user creates and uses; user data belongs to the user. Examples of user data include word processing documents, spreadsheets, or graphics files. Examples of user-accessed data that is *not* considered to be user data include database records that exist in a corporate database and documents that are shared by many users but that are not exclusively owned by any single user.

In a managed environment, user data is stored in files in the **My Documents** folder. Administrators can use Folder Redirection to redirect the paths of the following special folders to a network location to back up and protect the data: My Documents, My Pictures, Application Data, Desktop, and Start Menu.

User settings are the configuration choices — stored by the operating system or applications — that the user applies to a desktop or to applications. Typically, settings include variables such as the customized toolbar settings in an application, icon arrangement and color scheme of the desktop, mouse pointers, and language options. User settings are stored in the registry, the Application Data folder, on the Desktop, and on the Start Menu in the user’s user profile.

User Profiles

A user profile includes a user’s unique settings, such as printer connections, desktop icons, mouse settings, folder settings, and the special folders that can be redirected. (Table 7.2 lists the contents of each user profile folder.) A user profile is automatically created the first time that a user logs on.

A user profile consists of a *registry hive* and a *set of profile folders*.

Registry hive NTuser.dat in file form. It is loaded by the system at logon and mapped to the registry subtree HKEY_CURRENT_USER. NTuser.dat stores the user's registry-based preferences and configuration.

Set of profile folders Stored in the file system. User profile files are stored in the file system in %SYSTEMDRIVE%\Documents and Settings (for example, C:\Documents and Settings), in per-user folders. The user profile folder is a container for applications and other system components to populate with subfolders and per-user data, such as documents and configuration files. Windows Explorer uses the user profile folders extensively for the user's desktop, the **Start** menu, and the **My Documents** folder.

Table 7.2 Contents of the User Profile Folder

User profile folder	Contents
Application Data*	Program-specific data (for example, a custom dictionary). Program vendors decide what data to store in this user profile folder.
Cookies	User information and preferences.
Desktop	Desktop items, including files, shortcuts, and folders.
Favorites	Shortcuts to favorite locations on the Internet.
Local Settings*	Application data, history, and temporary files. The Local Settings folder and its subfolders do <i>not</i> roam with the roaming user profiles.
My Documents	User documents and subfolders.
My Recent Documents	Shortcuts to the most recently used documents and most accessed folders.
NetHood*	Shortcuts to My Network Places items.
PrinHood*	Shortcuts to printer folder items.
SendTo	Shortcuts to document-handling utilities.
Start Menu	Shortcuts to program items.
Templates*	User template items.

* These folders are hidden by default.

The three types of user profiles are *local*, *roaming*, and *mandatory*.

Local user profile The default profile type that resides only on the computer at which the user is logged on. A local profile is created whenever a user first logs on to a computer. Local profiles are highly recommended for users who never connect over fast links (such as remote users) or those who need their user settings to roam to whichever computer they use to log on.

Roaming User Profile Ideal for users who use different computers on the network and who need to have their customized settings and data available to them at each computer they use. A roaming user profile is copied to a specified server at logoff. When the user logs on to another computer in the network, the roaming user profile is copied from the server to that computer.

When the user logs off the second computer, the profile is copied back to the server, thus maintaining the most recent version of the profile on the server.

A mandatory user profile A profile that you create to provide specific settings for users. Any changes that users make to their desktop while they are logged on are lost when they log off. With Windows Server 2003, the recommended tool for establishing strict control over workstations is Group Policy, not mandatory profiles, because mandatory profiles are less manageable and more likely to create administrative problems.

Folder Redirection

Use Folder Redirection to relocate specific user folders to centrally managed shared folders on the network. You can redirect **My Documents**, **My Pictures**, **Application Data**, **Desktop**, and **Start Menu**. Users can then work with the files in those folders from any computer on the network, and the folders receive the benefits of centralized security and backup.

My Documents The standard folder in which user data is stored. By redirecting **My Documents** to a shared network server, the user can access all the documents from any computer. Also, important user data can be more easily backed up as part of routine system administration, requiring no action on the part of the user.

My Pictures The default location for pictures and images in Windows 2000. Typically, **My Pictures** is contained in the **My Documents** folder. By default, if **My Documents** is redirected, **My Pictures** is also redirected. Alternatively, **My Pictures** can be redirected independently of **My Documents**. However, it is recommended that you allow **My Pictures** to remain within **My Documents**, unless you need to separate these folders for a specific reason such as server scalability, for example.

Application Data A folder in the user's profile where applications often place large amounts of data (such as a custom dictionary). By redirecting the Application Data folder, users with roaming profiles can still access files in their Application Data folder without downloading those files every time they log on.

Desktop A folder that includes files and shortcuts.

Start Menu Windows Server 2003 allows Folder Redirection to redirect the Start Menu folder.

Offline Files

Offline Files is a feature that complements Folder Redirection and lets users disconnect from the network and work as if they were still connected. When the computer is offline, the files and folders appear in the same directory as they did online — as if they still resided in the same location on the network. This allows the user to edit files when they are disconnected from the network. The next time the user connects to the network, the offline changes are synchronized with the shared folder on the network.

Offline Files is a stand-alone technology. You do not need to pair it with Folder Redirection. However, using the technologies together works well. To ensure that users can access their files even when the network is unavailable, it is recommended that you use Offline Files along with Folder Redirection, especially if you are redirecting the Application Data folder.

Synchronization Manager

File synchronization ensures that local copies of offline files match their network counterparts. When using Offline Files, users can synchronize all network resources by using the Synchronization Manager. You can set the Synchronization Manager to automatically synchronize some or all resources. For example, users can set certain files and folders to be synchronized every time they log on or off the network. The Synchronization Manager quickly scans the system for any changes, and if it detects changes, the resources are updated. Only resources that have changed are updated.

User Profile Quotas

To specify the maximum disk space that a user profile can occupy, use the **Limit Profile Size** Group Policy setting. This setting is in the **User Configuration\Administrative Templates\System\User Profiles** node of the Group Policy Object Editor. When you enable this policy setting, you can set options that determine the maximum profile size, specify whether to include registry files when calculating the profile size, and define the user notification options. Profile quotas apply to all types of profiles.

For roaming user profiles, it is recommended that you use profile quotas to limit profile size, not disk quotas. If you use disk quotas to manage profile size, the users find out they have exceeded their quota *after* they log off. If you use profile quotas, the Proquota.exe tool displays a message to the users when they exceed their profile quota. Users can then manually select and delete files from one or more profile folders by using Windows Explorer or **My Computer**. Proquota.exe prevents a user from logging off from the network until the profile size is decreased. This tool is enabled when you set the **Limit Profile Size** policy setting.

Disk Quotas

Administrators can use disk quotas to track and manage disk space usage on the servers that contain users' redirected folders. Disk quotas apply to NTFS volumes. You can specify a disk quota limit and a disk quota warning level. For example, you can set a disk quota limit to 500 megabytes (MB) and the disk quota warning level to 450 MB. In this case, the user can store no more than 500 MB of files on the volume. You can configure the disk quota system to log a system event if the user stores more than 450 MB of files on the volume.

Remote OS Installation Feature

Administrators can enable remote installation of Windows 2000– and Windows 2003–based operating systems and desktop images on new or replacement computers. By using Remote Installation Services, you can direct client computers to a Remote Installation Services server and install automated, customized versions of the operating system. Administrators can use Group Policy to manage Remote Installation Services by centrally setting client configuration options. The remote OS installation feature uses Active Directory, Group Policy, the Dynamic Host Configuration Protocol (DHCP) service, and Remote Installation Services.

To facilitate computer replacement, you can use Remote Installation Services to install the operating system, Group Policy–based software installation to recover applications, Roaming User Profiles to restore user profiles, and Folder Redirection to manage files centrally.

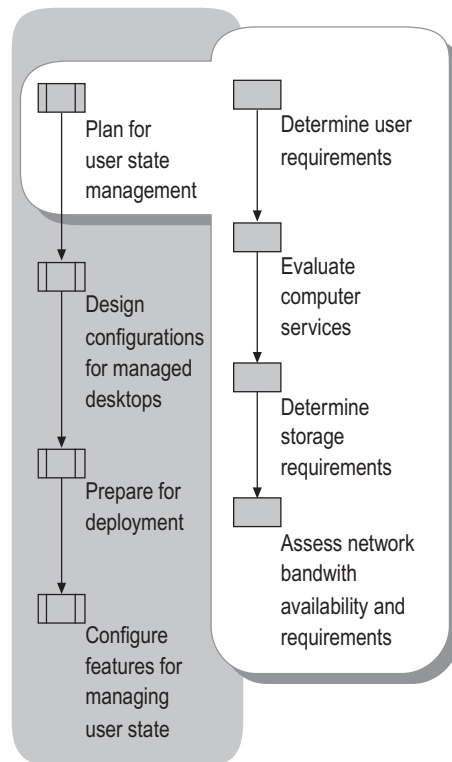
For more information about managing user profiles, Folder Redirection, Offline Files, and Synchronization Manager for Windows XP in a Windows 2000 environment, see the User Data

and Settings Management link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Planning for User State Management

During the planning stage of your implementation of user state management, you need to assess your current environment. Assessment includes determining your users' business needs and the types of computer roles in your organization; estimating disk storage requirements; and evaluating network bandwidth. Based on this information and the requirements of your organization — security, for example — you can define managed desktop configurations for the various user and computer groups. Figure 7.2 illustrates the planning process.

Figure 7.2 Planning for User State Management



Determining User Requirements

Typically, larger organizations have a wide range of user needs. In addition to knowing your organization's needs, you must understand the work needs of users before you design and deploy services that define the users' computing environment.

When you plan a deployment, determine the following:

- The number of users to be accommodated. Allocating resources, such as disk space and network bandwidth, varies depending on the numbers of users.
- The primary applications and computing services in use, such as databases and e-mail. Databases are stored in shared folders on the network and do not move with users. However, users typically have user settings that must be available to them wherever the users log on to. E-mail applications might store users' e-mail folders in network shares or on the local workstation. In either case, these folders must remain available.
- Whether mobile users switch from one workstation to another or use a single portable computer. Users who switch between workstations benefit from roaming user profiles more than those who work exclusively on a single computer.
- The security requirements of different users, applications, and data files. Security involves access controls and backup requirements.

To develop a plan for managing user data and settings, categorize users according to their job types and computer experience. Then, determine whether users need to be able to work from any computer on the network and retain access to network-based files when they are not connected to the network.

For more information about user categories, see “Planning a Managed Environment” in this book.

For job aids to assist you with the deployment processes discussed in this chapter, see Additional Resources later in this chapter.

Evaluating Computer Services

For the purpose of managing computers, determine whether a specified computer offers the following services:

- Supports logging on by different users
- Retains or discards user profiles between user sessions
- Provides local data store for offline file copies

Determining Storage Requirements for Users, Local Workstation, and Servers

To plan for disk space allocation, you need to determine the typical disk storage requirements of the users and computers in your organization.

User Storage Requirements

User settings typically require about 10–20 MB of storage space per user, and they are simple to plan for. User data size is typically more varied, and planning its management involves multiple factors.

Local Workstation Storage

The IntelliMirror technologies provide a wide range of options for configuring your data storage. The options you select have associated costs in hardware and computing overhead as follows:

- Some Group Policy configurations leave copies of roaming user profiles on workstations. This reduces logon delays, but as the number of users who share a workstation increases, the disk space that is devoted to user profile storage increases. The performance improvement typically outweighs the additional workstation storage requirements, but you have to plan for residual profile storage space.
- Redirecting large folders (My Documents, for example) out of the user's profile reduces the local disk space that is required by the user's profile. Redirecting My Documents to a shared folder on the network and leaving My Pictures in My Documents is the best option for most users.
- Implementing Offline Files on a workstation requires space for the offline file cache and the Offline Files database. Manual selection of specific files or folders for offline caching improves reliability of access to critical information while ensuring offline caches are no larger than necessary.

Server Disk Storage

Estimating the amount of server storage space to allocate for user data and profiles depends in part on understanding local workstation disk storage requirements. First, determine how much disk space is currently occupied by users' data and, separately, by users' profiles.

You can use the Diruse.exe command-line tool that is included with the Windows Support Tools to gather disk usage information, such as how much disk space each folder uses in a directory tree on a disk volume. For information about how to use the **Diruse** command, type `diruse/?` at the command line. You can install the Windows Support Tools from the Windows Server 2003 CD. In the \Support\Tools folder, double-click **Suptools.msi** and follow the instructions that are displayed on the screen.

To prevent large folders from being unnecessarily copied across the network along with the rest of the roaming profile when a user logs on, redirect My Documents and My Pictures. This reduces the roaming profile size substantially because redirected folders are not stored or copied as part of the roaming profile.

To exclude additional folders from the user's profile, you can use the **Exclude directories in roaming profile** policy setting. This setting is in the **User Configuration\Administrative Templates\System\User Profiles** node of the Group Policy Object Editor. This policy blocks specified folders from roaming.

You also need to estimate the amount of server disk storage that you need for user data and profiles.

Estimating server disk space for user data and profiles example

You have 5,000 users who can benefit from Redirected Folders. Of these, 4,000 users also need roaming user profiles. You have determined that the average amount of disk space used for each user's personal files is 80 MB. You have also viewed the technologies available for roaming user profiles and found that a typical roaming user profile uses 15 MB. In this situation, you need approximately 400 GB disk space for user data and 60 GB disk space to store roaming user profiles. To provide a small margin, add 50 percent to these numbers, for a total disk storage requirement of approximately 600 GB for user data and 75 GB for user profiles.

Investigate profile sizes in your organization to determine average and maximum sizes for your own users' profiles. A typical disk-quota setting for users is about 200 MB. Due to the wide variation in disk-space requirements of users, disk quotas often require a lot of adjustment. For more information about establishing disk quotas, see "Configuring Disk Quotas on NTFS Volumes" later in this chapter.

You can control the maximum size of a user's profile by using Group Policy. If a user profile exceeds the allocated size, the user must reduce the size of the profile to log off. Restrictions for profile size apply to both local and roaming profiles. For more information, see "Setting Quotas on User Profiles" later in this chapter.

Assessing Network Bandwidth Availability and Requirements

The availability of network bandwidth can affect how Group Policy settings are applied. By default, some policies do not process across a slow network connection. If the network link speeds between a client and the authenticating domain controller fall below the default slow-link threshold of 500 kilobits per second (Kbps), only the administrative template (registry-based) settings and security settings are applied. By default, all other Group Policy settings, including Software Installation and Folder Redirection, are not applied. When the available bandwidth between the client and the domain controller falls below this preset threshold, the client is said to be on a slow link.

If necessary, you can modify the default slow link behavior by using the **Group Policy slow link detection** policy setting for both the user and computer aspects of a GPO. The **Group Policy slow link detection** policy setting is available in both **Computer Configuration** and **User Configuration**, under the **Administrative Templates\System** node. You can also adjust the Group Policy extensions that are processed below the slow link threshold. However, depending on your situation, it might be more appropriate to place a local domain controller at a remote location to serve your management requirements.

For more information about slow links, see "Designing a Group Policy Infrastructure" in this book. For more information about Group Policy mechanics and infrastructure, see the *Distributed Services Guide* of the *Windows Server 2003 Resource Kit* (or see the Distributed Services Guide on the Web at <http://www.microsoft.com/reskit>).

Is it important to have sufficient network bandwidth available between servers and workstations when you deploy Roaming User Profiles, Offline Files, and Folder Redirection. It is also

recommended that the servers to which workstations connect for this data are on a fast network link. Check your network configuration for ways to minimize network routing hops when accessing frequently needed data. Keeping the needed data and the user on the same subnet improves performance.

When evaluating network bandwidth for Folder Redirection, be aware that slow link detection is based on link speed between the workstation and the domain controller to which the workstation is connected. If the link to the domain controller is fast but the link to a shared folder that contains redirected folders is slow, users might experience slow performance when accessing redirected files. Selecting these redirected files for offline caching does not improve file access speed in this case because the slow link is not detected. As a result, the Offline Files cache is not brought online.

Logging on the first time after having a folder configured for redirection might be slow for the user because all the files are being copied from the user's local drive to the shared folder on the network. The time this takes depends on the amount of data being copied, the local computer's disk I/O speed, the available network bandwidth, and server performance. You can minimize logon time by doing the following:

- Locate the validating domain controller in close proximity to the workstations that it needs to validate.
- Simplify or remove existing user logon scripts. Group Policy can replace many conventional logon script settings. Group Policy creates additional download time at logon; however, this is insignificant if Group Policy objects (GPOs) are judiciously used (keeping in mind that the number of GPOs influences logon time). If Group Policy is used for new folder redirection or software installation, logon time for those actions increases.
- Keep roaming user profiles as small as possible. Folder Redirection and profile quotas are common tools to manage roaming user profile size. For more information about managing roaming user profile size, see "Recommendations for Folder Redirection and "Setting Quotas on User Profiles," later in this chapter.

Understanding network traffic can help you design your network and servers to balance network loads. In some cases, it is cost effective to add another server or subnet to redistribute load; in other cases, making simple changes to server configuration can produce similar benefits.

Designing Configurations for Managed Desktops

You can use IntelliMirror and Group Policy to design well-managed desktops that enhance user and computer efficiency. To take full advantage of these benefits, it is recommended that you define and set up default user configurations.

A managed desktop configuration must be carefully adapted to the target users' applications, tasks, and locations. It can also increase productivity by preventing users from making system

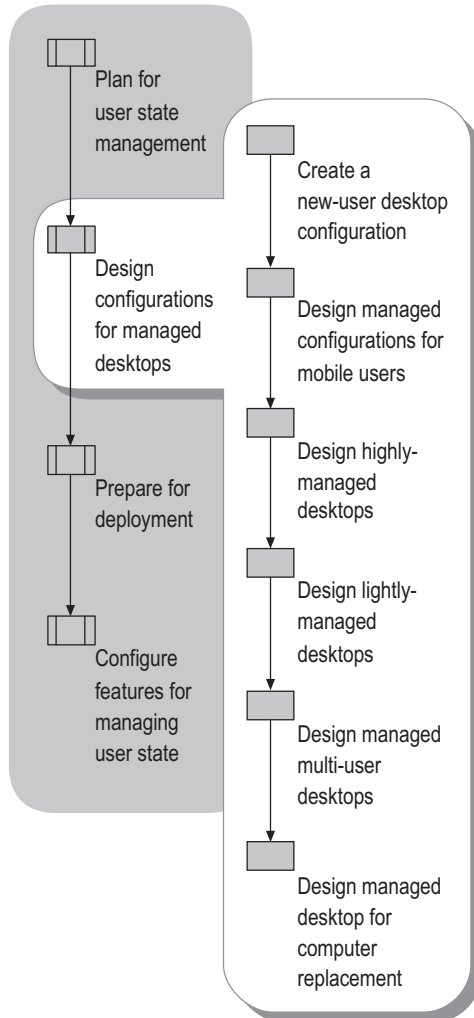
changes that can cause downtime. By establishing managed configurations, you make troubleshooting or replacement easier and reduce the cost of support.

IntelliMirror and Group Policy are designed for environments where administrators need to centralize tasks such as the following:

- Managing new users
- Managing mobile users
- Creating lightly managed desktops
- Creating highly managed desktops
- Managing multi-user desktops
- Replacing computers

Figure 7.3 describes the process for deploying managed desktop configurations that you select.

Figure 7.3 Designing Managed Desktop Configurations



For more information about user and computer types and their management, see “Planning a Managed Environment” in this book.

Creating a New User Desktop Configuration

IntelliMirror, Group Policy, Windows Installer, and Remote Installation Services significantly streamline adding new users and their computers to your network. You can use these technologies to add a new managed user.

Example A new user logs on to a new computer and finds shortcuts to documents on the desktop. These shortcuts link to common files, data, and URLs such as the employee handbook, the company intranet, and appropriate departmental guidelines and procedures. Settings such as desktop options, application configurations, and Internet settings are configured to your

organization's standard. As users customize their personal desktop environment (within boundaries you define), their changes are added to the initial environment. For instance, the user might change the screen resolution for better visibility or add shortcuts to the desktop.

In the preceding example, a default domain profile and Group Policy are used to configure the new user's environment, based on job requirements. The advantage of using a default domain profile is that all new users start from a common, administrator-defined configuration in an existing domain structure. You create a customized domain profile that applies to all new domain users the first time they log on, and they receive the customized settings from this profile. Then, as a user personalizes desktop settings and items, the new settings are saved in the user's profile that is stored locally, or in the case of a roaming user profile, in a predetermined location on the network. By implementing a default domain profile in conjunction with roaming user profiles, you provide users with the necessary business information as a starting point and also allow them to access their settings whenever and wherever needed. Finally, you can use Folder Redirection to redirect a user's My Documents folder to a network location, so that the user's documents are securely stored on a network server, which can be backed up regularly.

The administrator uses the Software Installation extension of Group Policy to assign Microsoft® Word to a user or a specific group of users. The new users log on for the first time and see that the software required to do their jobs is listed on the Start menu. When the user selects Microsoft Word from the Start menu, or double-clicks a Word document, Windows Installer verifies that Word is installed on the local computer. If it is not, Windows Installer downloads and installs the necessary files for Word to run and sets up the necessary local user and computer settings for on-demand installation.

For more information about Software Installation, see "Deploying a Managed Software Environment" in this book. For more information about Windows Installer, see the *Distributed Services Guide* of the *Windows Server 2003 Resource Kit* (or see the "Distributed Services Guide" on the Web at <http://www.microsoft.com/reskit>).

Designing Managed Configurations for Mobile Users

Many organizations have *mobile users* — traveling employees who often use portable computers. Typically, mobile users log on to the same computer. Sometimes they connect by using a high-speed line and sometimes by using a low-speed (or dial-up) line. Some mobile users never have a fast connection. Mobile users fall into two main categories:

- Users who spend the majority of time away from the office or have no fixed office. Typically, these users connect by using slow links, although they might have occasional LAN access to their logon server, data servers, and application-delivery servers.
- Users who spend most of their time in an office but occasionally work at home or in another location. The majority of their network access is at LAN-speed, but they occasionally connect by using remote access or remote network links.

Despite the apparent differences between these two types of users, you can often accommodate them with a single configuration. However, you might want to create a slightly different GPO for users who spend the majority of their time out of the office.

Mobile users are often expected to provide much of their own computer support because on-site support is not available. For this reason, you might want to elevate those users' permissions so that they can install printers, for example.

However, you can also restrict mobile users from making system changes that might damage or disable their computers. For example, you might restrict mobile users from altering certain Internet Explorer settings or adding unapproved hardware devices. If those users need access to some MMC administration snap-ins, you can make a restricted set of those tools available to them.

Mobile users expect transparent access to the most critical parts of their data and settings even if their portable computer is not connected to the network. For example, they roam to desktop computers while their portable computer is in use to read mail while they are in a remote office. Finally, mobile users frequently disconnect their portable computer from the network without logging off and shutting down. This is more likely to happen when they use the hibernate and standby features of Windows XP Professional.

IntelliMirror provides several tools that simplify managing mobile users. By using the management tools of user data and settings, users can work on files offline and automatically update network versions of those files when they reconnect to the network. By using the Offline Files feature, users can work on network files when they are not connected to the network. Synchronization Manager coordinates synchronization of any changes between the offline version of a file and the network version.

**Note**

If users are likely to disconnect from the network without logging off, it is recommended that you set Offline Files to periodically synchronize in the background. If Offline Files is set to synchronize only when users log off, users' files might not be current. You might also want to educate users to manually synchronize their data before disconnecting from the network to ensure that all files are current.

Synchronization Manager also helps manage multi-user network files. If multiple users modify the same network file, Synchronization Manager notifies the users about the conflict and offers several resolution methods. The users can save the network version, their local version, or both versions. If both are to be kept, the user is asked for a new file name to store one of the versions so that uniqueness is maintained.

Software Installation for mobile users requires some additional planning. You can make sure that all important software components, defined by you or the user, are completely installed initially. This allows users to access the necessary software even when they are not connected to the network. That means that prior to these users leaving the office, you must ensure that all relevant features within the application are installed locally and are not just advertised. For example, make sure the spelling checker for Microsoft® Office is locally installed so that the user does not trigger on-demand installation of this feature while offline.

It is not recommended that you publish software for mobile users who connect over slow links. Additionally, when mobile users connect over a slow link, user-assigned software effectively behaves the same as if you published it for these users. If you set the Group Policy slow-link detection setting to the default in the user interface, the software is not installed on demand. However, in the Group Policy setting for slow-link detection, you can define the connection speed that you consider to be a slow link.



Note

It is recommended you treat any link that is slower than local area network (LAN) speed as a slow link.

If you determine that it is appropriate for mobile users to download software from a remote location and they experience difficulty staying connected when downloading the software, you can verify that the connection speed and Group Policy settings are set appropriately in the **Group Policy slow link detection** setting in **Computer Configuration/Administrative Templates/System/Group Policy** or **User Configuration/Administrative Templates/System/Group Policy**.

Typically, a mobile user has a single portable computer and does not roam between portable computers (unless the computer is replaced). However, roaming user profiles give some protection against the failure or loss of a portable computer and allow a user to roam to a desktop computer to connect to a fast network. If the mobile user is *not* often connected to a fast network, it is better not to use roaming user profiles.

Data accessed by the mobile user typically falls into one or more of the following categories:

- Data that resides on a network server and that users want to access while not connected to the network. Users typically own this data (for example, their home directory), but shared data can also be stored on the local computer.
- Data that resides only on the network server (either not needed offline or volatile shared data that is inappropriate for storing offline).
- Data that resides only on the portable computer hard disk. Examples are policy manuals or other read-only items or large document sets that are needed offline by the user but the performance overhead of synchronizing precludes storing them on a file server. (In this case, a suitable backup mechanism is definitely needed.) Other examples are large database files or other data items that have their own synchronization mechanism, such as the offline storage feature in Microsoft® Outlook® messaging and collaboration client.

Table 7.3 summarizes desktop management features that you can use to create a mobile user configuration.

Table 7.3 Features of a Mobile User Configuration

Feature	Explanation
Folder Redirection	Use to redirect the My Documents folder. This allows users to access centrally stored data and documents from anywhere. Redirected folders are automatically made available offline, to provide access when users are not connected to the network.

Ability for user to customize	Permit customization within certain guidelines. You can allow users to personalize their work environment but still prevent them from making changes to critical system settings.
Software Installation	Core applications are installed on all laptops (these applications are assigned). Optional applications are available for users to install locally (these applications are published).
Group Policy Settings	Use Group Policy settings to create the managed environment.

Recommendations for Configuring Mobile Users Computers

Typically, a mobile user works offsite, connects to the corporate network over a slow link from various locations, and occasionally connects to the network by using a fast link. This user also uses a desktop computer at the home office, so it is preferable that the user's portable computer and desktop computer have the same settings. To provide a consistent user experience, follow the guidelines in this section for configuring user profiles.

When configuring multiple mobile users, set up an OU for mobile computers and apply the same settings to all users in that OU.

User Profile

The following suggestions can guide you in planning user profile configurations for mobile users:

- If the users regularly connect to the network by using a fast link, and you want to back up their state or if they use multiple computers, use a roaming user profile.
- If the users rarely connect by a fast link, use a local profile.
- If users roam to LAN-connected computers in the domain and also have portable computers, use a roaming user profile. For portable computers, enable the **Only allow local user profiles** policy setting which is available in the **Computer Configuration\Administrative Templates\System\User Profiles** node of the Group Policy Object Editor. Note that a Computer Configuration Group Policy setting takes precedence over a User Configuration setting, so the user receives the user setting on a desktop computer and the computer setting on the portable computer.

Roaming User Profiles

By default, roaming user profiles do *not* roam over slow links. It is recommended that you configure roaming user profiles only for mobile users that log on *frequently* over a fast link, so that their profiles are saved to the server. This provides backup of the user state. However, if the user *never* logs on to the network over a fast link, or does so infrequently, it is *not* useful to provide roaming user profiles for that user.

Folder Redirection, Offline Files and Slow Links

If mobile users frequently connect at high speed, Folder Redirection and Offline Files are beneficial for backup and synchronization. By default, Folder Redirection and Offline Files are *not* applied over slow links. You can override the default by using the **Group Policy Slow Link**

Detection policy setting. This setting is in the **User Configuration\Administrative Templates\System\Group Policy** node of the Group Policy Object Editor.



Important

If you change the default setting for Group Policy slow-link detection, all group policies are affected, and all Group Policy settings are applied over a slow link, including policies that install software. This is not appropriate for most users.

Designing Highly Managed Desktops

Typically, a highly managed desktop is the most appropriate workstation configuration for users in an office environment. Users' personal files are cached locally, so they are available if a server becomes unavailable. Authoritative versions of the files are retained on central servers, so backup and physical security are easier to protect. The user's personal configuration and customizations are stored on central servers, so replacing a workstation does not alter a user's computing environment. Also, users can receive their own personal computing environment on another user's workstation. After the visiting user logs off, and the regular user logs on, the regular user's personal computing environment is restored. To implement this process, you must configure Roaming User Profiles, Folder Redirection, Offline Files, and server disk quotas.

To create highly managed desktops, perform the following tasks:

- Set up Folder Redirection to redirect My Documents to a shared folder on the network.
- Set up Roaming User Profiles for users who use multiple computers so that their settings follow them to any computer they use. For more information about implementing roaming user profiles, see "Using roaming user profiles" in Help and Support Center for Windows Server 2003.
- Set up Offline Files to minimize vulnerability to network status inherent in redirected folders. Designated files are cached locally to ensure that in the event of network disconnection, users can continue to work on these important files. For more information about using Offline Files to minimize vulnerability to network status, see "Configuring Offline Files" later in this chapter.
- Set up Disk Quotas on the servers that contain redirected folders so that individual users cannot use too much disk space.
- To remove cached versions of roaming profiles when the users log off, apply the **Delete cached copies of roaming profiles** policy setting. This policy setting is available in the **Computer Configuration\Administrative Templates\System\User Profiles** node of the Group Policy Object Editor.

- Make applications available to users by using Group Policy–based software management to assign or publish applications to users. You can also use Microsoft Systems Management Server to manage software if your organization is medium or large, if your users run operating systems earlier than Microsoft® Windows® 2000 Professional, or if you require more advanced capabilities for planning, distributing, and tracking software.

For more information about managing software, see “Deploying a Managed Software Environment” in this book.

For more information about Systems Management Server, see the SMS Product Information link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Designing Lightly Managed Desktops

Lightly managed workstations are often a good solution for advanced users, such as software developers, who require a lot of control over their computers. To implement a lightly managed workstation, perform the following tasks:

- Set up Roaming User Profiles for users, so that their settings follow them to any computer they use.
- Set up Folder Redirection and Offline Files. Any files that are redirected must be set as Offline Files, so that the users can continue to work on their important files in the event of network disconnection.
- Set up Disk Quotas on the servers that contain redirected folders so that individual users cannot exhaust available shared disk space.

Designing Managed Multi-User Desktops

A multi-user desktop is a managed desktop that many users can use. In this configuration, users can partially configure the desktop. The multi-user desktop is ideal for computers that are set up for public access, such as computers in a library or school. The multi-user desktop gets heavy traffic and must be reliable and unbreakable. It must also be flexible enough to allow some customization. For example, students might need access to customized applications for instructional purposes and need to install applications that the network administrator publishes. You might also want to allow users to change their desktop wallpaper and color scheme.

However, you need to control the configuration of hardware and connection settings to maintain security. Multi-user computers often require certain tools, such as word processing software, spreadsheet software, or a development studio.

With the multi-user desktop configuration, users can do the following tasks:

- Modify Internet Explorer and the desktop
- Run assigned or published applications
- Configure some Control Panel options

However, users cannot:

- Use the **Run** command on the **Start** menu or at a command prompt.
- Add, remove, or modify hardware devices.

In the multi-user environment, a user is unlikely to return to the same computer. Therefore, local copies of roaming user profiles that are cached on the computer are removed after the user logs off if the roaming user profile settings are successfully synchronized back to the server. Roaming user profiles use the My Documents and Application Data folders that are redirected to a network folder. However, users can log on even if their network profile is not available. In this case, the user receives a temporary profile that is based on the default profile.

The multi-user computer is assigned a set of core applications that is available to all users who log on to that particular computer. In addition, a wide variety of applications can be assigned to or published for users. Users cannot install from a disk, a CD-ROM, or an Internet location. To conserve disk space on the workstation, most applications must be configured to run from a network server. Start menu shortcuts and registry-based settings are configured when the user selects an application to install, but most of the files that are associated with an application remain on the server. The shared folders that store the applications can be configured for automatic caching for programs so that application files are cached at the workstation on first use.

Table 7.4 shows the desktop management features that are used to create a multi-user computing environment.

Table 7.4 Features of a Multi-User Desktop Configuration

Feature	Specifics	Explanation
Multiple users	Per-user logon accounts	Users share this computer at different times. Each user has a unique logon account.
Roaming User Profiles	Yes	User settings are available from any computer and administrators can easily replace computers without losing their configuration. When the user logs off, the local cached version of the profile is removed to preserve disk space.
Folder Redirection	My Documents, Desktop, and Application Data folders	User data is saved in shared folders on the network, and Group Policy prevents users from storing data locally.
Ability for user to customize	Some	Most of the system is locked down, but some personal settings are available.
Assigned applications	Multiple	Core applications that are common to all users are assigned to the computer. Other applications are available for on-demand installation by means of user assignment.
Published applications	Multiple	Applications are available for users to install from Add or Remove Programs in Control Panel.

Group Policy settings	Yes	Group Policy settings are used to create the managed environment.
-----------------------	-----	---

Designing Managed Desktops for Replacing Computers

When a user receives a new or different computer, it can cause a time-consuming interruption in productivity. It is important that users regain productivity in the shortest possible time and with a minimum of support. This can be accomplished by storing user data and settings independently of any specific computer. By using the Group Policy features Roaming User Profiles and Folder Redirection, you can ensure that the user's data, settings, and applications are available wherever the user logs on to the network.

To further simplify setting up a new managed computer on your network, use Remote Installation Services to create standardized operating system configurations. Remote Installation Services allows you to create a customized image of a Windows XP Professional or Windows 2000 Professional desktop from a source computer. Then, you can save that desktop image to the Remote Installation Services server. The image can include the operating system alone or a preconfigured desktop image, including the operating system and a standard, locally installed desktop application. You can use that preconfigured image to set up multiple desktops, saving valuable time. Create as many standard desktop images as you need to meet the needs of all types of users in your organization. For more information about using Remote Installation Services, see the Remote Installation Services (RIS) link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

These IntelliMirror technologies can work together when a computer fails, as the following example illustrates.

- **Example.** A user's computer suddenly undergoes a complete hardware failure. The user calls the internal support line. Presently, a new computer, loaded only with the Windows XP Professional operating system, arrives. Without waiting for technical assistance, the user plugs in the new computer, connects it to the network, starts it, and can immediately log on.

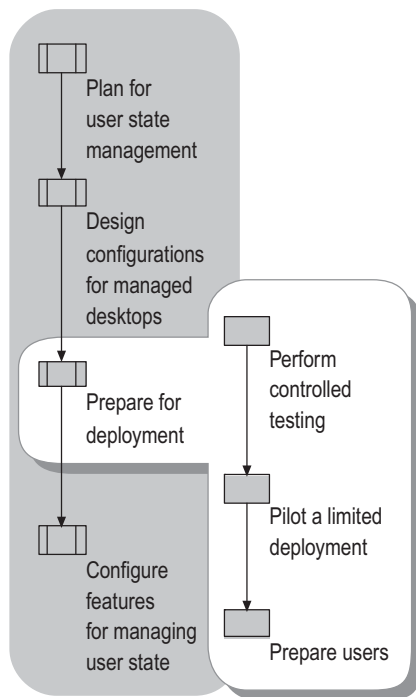
Because roaming user profiles are enabled, the user finds that the desktop takes on the same configuration as the computer it replaced — the same color scheme, screensaver, and all the application icons, shortcuts, and favorites are present. Because Folder Redirection and Software Installation are enabled, the user can access data files on the server after the appropriate applications are automatically installed.

Preparing for Deployment

You can minimize expense, effort, and user inconvenience by implementing your deployments in phases. You can further prepare for user satisfaction by communicating clearly to your users the deployment plan and schedule.

The IntelliMirror tools for managing computing environments for users are powerful, and they can have unwanted consequences if applied incorrectly. Therefore, it is essential that you thoroughly test all your deployments of Group Policy and User Data and Settings before you deploy them on a large scale. Figure 7.4 highlights the process of preparing for deployment of your design.

Figure 7.4 Preparing for Deployment



Performing Controlled Testing

After you choose the IntelliMirror technologies to deploy, set up a test environment to thoroughly test your configurations.

For testing, you typically need a domain controller, a file server, two or more workstations, and possibly a mobile computer that is connected by a slow link. These requirements might increase depending on the scale at which you want to test your proposed configuration. Build on these recommendations until you have included all of the requirements for your organization.

Piloting a Limited Deployment

After you complete tests in a controlled environment, you are ready to conduct a pilot deployment to expose and resolve unexpected problems before you deploy on a large scale. Keep the group of users that you select for your pilot deployment to a manageable number (10 to 20).

On the first day of your pilot deployment, modify one or two user accounts from a single group. On the second day, after resolving any new problems, apply the configurations to 10 or 20 users in that group. Expand the pilot deployment gradually.

Preparing Users

The deployment of user data management and user settings management policies is more noticeable to users than the deployment of many other technologies because those settings directly affect the look and use of users' desktops. Users who know what to expect from a deployment are better prepared to deal with temporary inconveniences and alterations in their work environment. Pilot users can help you inform other users to help them adapt to changes in their work environment. Having pilot users share their understanding and expertise throughout your user community improves overall user satisfaction and reduces the number and cost of technical support calls.

Teaching Users about Roaming Profiles

Typically, roaming user profiles require very little user training. Users who connect to the network over a LAN appreciate seeing the same desktop settings when they log on to any computer. Users need only a few common concepts to understand roaming profiles.

Logging on to and off from more than one computer

When a user with a roaming user profile uses multiple computers simultaneously, the settings from the last time a user logs off from the computer are preserved. This means that if a user is logged on to two computers simultaneously, the user should log off *last* from the computer whose configuration the user wants to preserve. *Only* the last copy of the user profile is preserved.

Roaming user profiles on a fast network link only

By default, roaming user profiles roam over a fast network link only. Users cannot receive their roaming user profiles over a slow link, as a message explains to them. If users do not need to see the message, you can use Group Policy to disable it, or you can set the **Timeout for dialog boxes** policy setting in the Group Policy Object Editor to 1 to make it less noticeable. (This setting is in the **Computer Configuration\Administrative Templates\System\User Profiles** node of the Group Policy Object Editor.)

Educate users to keep their profile size to a minimum. For example, they can save shortcuts to documents on their desktop instead of saving the actual document. If you use the **Limit profile size** policy setting to manage profile sizes, teach users how to respond to the messages they receive when they exceed that limitation. If you force users to reduce their profile size before logging off, show them how to do so safely. The **Limit profile size** policy setting is available in the **User Configuration\Administrative Templates\System\User Profiles** node of the Group Policy Object Editor.

Teaching Users about Folder Redirection

If users are accustomed to seeing their documents in the My Documents folder, when you deploy Folder Redirection, most applications (such as Microsoft Word) appear and use the files in the same manner as they did before you redirected the folders.

Folder Redirection and remote access to another domain

When users connect to the network by using remote access and their computer accounts are not a part of the domain to which they are connecting, they need to know the full Universal Naming Convention (UNC) path to the shared folder that contains their files. For example:

`\\Servername\Redirected Folders\%username%\My Documents.`

The logon process might access one or more files from a redirected My Documents folder during a dial-up session.

Teaching Users about Offline Files and Synchronization Manager

When files are modified offline by more than one user, file conflicts can occur. Offline files are referenced to a specific version of the corresponding file on the server. When a file is modified offline, it replaces the server version of that file when the user reconnects to the network. Synchronization Manager checks the server version of the file to determine if it has changed since it was last synchronized.

If the server version of the file has not changed, the local copy of the modified file is copied to the server. If the server version of the file has changed since it was last synchronized, Synchronization Manager displays the **Resolve File Conflicts** dialog box. The user is offered the following options for dealing with multiple versions of the file.

Keep both versions Both versions of the file are saved to the server. The user name and a version number are appended to the local file name. For example, Report.txt becomes Report (John Doe v1).txt.

Keep only the version on my computer The local file replaces the server file.

Keep only the network version The server file replaces the local file.

View: Network Version Open and view the server version of the file.

View: Local version Open and view the local version of the file.

Typically, it is a good practice to minimize the number of users who can modify a file that is available offline. This practice prevents data loss and multiple file versions. The user can use Windows NTFS permissions to specify who can access the files. Grant *Change* permissions to users who are allowed to modify the file offline and *Read* permissions to users who need the data to be available while they are offline. Permissions still apply when users are offline.

Tell users that when the status of their network connection changes, an **Offline Files** icon appears in the notification area, and a message is displayed over the icon to notify users of the change. Users can continue to work with their files without interruption. For more information about the status of their connection, they can click the **Offline Files** icon in the notification area.

Teaching Users about Disk and Profile Quotas

If you implement disk or profile quotas, tell your users what to expect if they exceed their quotas and how to resolve the situation. Tell them how to request a quota increase. Make sure users know how to determine how much disk space they have used and how much they have left.

When a user tries to exceed a quota on a disk volume, the disk volume appears to be full. Any files that the user cannot save to that disk volume can be saved to an alternate disk volume to which they have access.

A user who exceeds a profile quota cannot log off until the profile size is reduced to the quota allowance. The user must remove files from the roaming user profile until the combined size of the redirected folders in the user's roaming profile drops below the profile quota.

Configuring User State Management Features

While the Folder Redirection, Roaming User Profiles, and Offline Files technologies are complementary, they are functionally independent. You can apply them either in combination or one at a time. The preferred method is to use these technologies in Active Directory environments with Group Policy because this approach provides the full benefits of IntelliMirror.

Using Active Directory and Group Policy to implement the IntelliMirror technologies helps you accomplish the following tasks and responsibilities:

- Centrally create and manage desktop configurations for all users and computers in your organization.
- Allow users to access their files from any location at any time by using Roaming User Profiles and Folder Redirection in combination with Offline Files.
- Manage how software is deployed and installed on computers to ensure that users have the software that they need to perform their jobs.
- Manage and enforce centralized data storage. This helps you keep important corporate data backed up.
- Replace computers efficiently by using the following technologies:
 - Remote Installation Services and Group Policy–based software installation to replace applications
 - Roaming User Profiles to recover user profiles
 - Folder Redirection to centrally store files

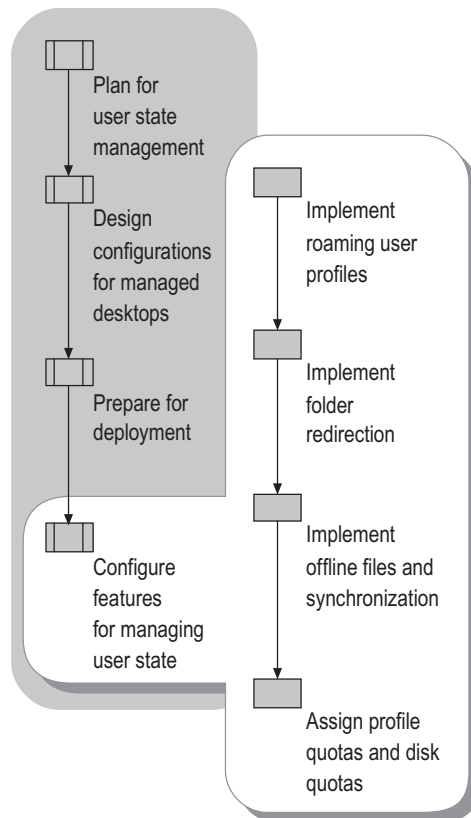
As you determine which technologies to deploy, consider how the deployment of one technology, such as Roaming User Profiles interacts with another, such as Folder Redirection. For example, redirected folders are not copied back and forth with Roaming User Profiles.

Implementing Folder Redirection before implementing Roaming User Profiles provides two benefits:

- Converting users profiles from local to roaming causes new logon delays because folders that were previously local are copied from a shared folder on the network during logon.
- Redirecting **My Documents** before implementing Roaming User Profiles ensures that the **My Documents** folder is never copied back and forth during a logon session. This also ensures that copies of **My Documents** that are left in profiles from previous logon sessions do not remain on workstation hard drives.

Figure 7.5 shows the processes you use to implement the user state management features that you select.

Figure 7.5 Implementing User State Management Features



Implementing new technologies in phases has a significant advantage: Testing is simpler. Because you have introduced fewer variables in each phase, it is easier to trace unexpected results back to their source.

It is important to include in your plan adequate time for testing the technologies that you intend to implement so that you can prevent problems. For more information about testing, see “Preparing for Deployment” earlier in this chapter.

Implementing the IntelliMirror deployment plan entails selecting group policies for GPOs and then applying those Group Policy objects to selected groups of users or computers. For more information about working with GPOs, see “Designing a Group Policy Infrastructure” in this book and the Group Policy topics in Help and Support Center for Windows Server 2003.

For information about managing desktops in environments that do not use Active Directory, see “Desktop Strategies for Computers Running Windows 2000 and Windows XP Without Active Directory,” later in this chapter.

Implementing Roaming User Profiles

You can reduce setup time, improve consistency, and simplify manageability of your user accounts by creating a default profile for each group of users, defined by their organizational function or role. For example, field engineers who primarily connect from remote locations and accountants who work exclusively on site are likely to benefit from different policy settings. You can start by customizing one profile to fit the general needs of users in a domain and then set the customized profile as the domain default user profile. Thereafter, you need only modify your default profile as needed for each group.

Recommendations for Roaming User Profiles

The following guidelines and recommendations for customizing roaming profile settings for your deployment include considerations for users roaming between different versions of the Windows operating systems.

Considerations for users roaming between different versions of the Windows operating systems

The following guidelines apply to roaming users who roam between computers running any of the following operating systems: Windows Server 2003, Windows 2000, and Windows XP:

- If you can avoid roaming between versions of the operating system, it is preferable that you do so. There is nothing inherent in roaming that causes problems, but the data that the applications put in the profile might cause unintended side effects on other versions of the operating system.
- Install the same application versions on all client computers.
- Make sure that the applications are installed using the same path and drive on all client computers.
- Make sure that the different versions of the operating system are installed on the same %systemdrive% and in the same %windir% location on all clients.

- If users roam between Microsoft® Windows® NT 4.0–based clients and Windows XP–, Windows 2000–, or Windows Server 2003–based clients, consider setting the profile path during the installation of Windows XP, Windows 2000, or Windows Server 2003. Differences in the default profile path (%windir%\Profiles versus %systemdrive%\Documents and Settings) may cause problems for users that roam between Windows NT 4.0–based clients and Windows XP–, Windows 2000–, or Windows Server 2003–based clients. To minimize the chance of problems, make sure the path to the profile is the same on all clients.

Redirect My Documents out of user's roaming profile

To reduce logon delay, use Folder Redirection to relocate large folders, such as **My Documents**, to shared folders on the network. Redirected folders are not copied as part of the Roaming User Profile during logon or logoff.

Do not use Encrypting File System with roaming user profiles

Encrypting File System (EFS) is *not* compatible with files in roaming user profiles. If you use EFS to encrypt profile folders or files, the user's profile does not roam.

Do not place roaming user profiles on a server volume that uses NTFS compression

It is recommended that you do not place user home folders and roaming profiles on a volume that uses NTFS compression. The frequent file creation and deletion can cause a compressed volume to become fragmented.

Combine Roaming User Profiles with Folder Redirection

When a user gets a roaming user profile, the data and settings that are stored in the user's local profile directories become mobile. The profile data is stored on a server and copied to a workstation when the user logs on. Storing this data on servers simplifies data backup and security. However, because large folders, such as **My Documents**, are copied, there can be logon delays. You can avoid these delays by using Folder Redirection in combination with Roaming User Profiles.

When a user profile folder is redirected to a shared folder on the network, the folder is no longer part of the user profile. While other profile data is copied to the local workstation when the user logs on, the redirected folder remains on the server and is accessed over the network.

Do not set disk quotas too low for users with roaming profiles

For users who have roaming user profiles, set the disk quota limits high enough to allow the system to create a temporary duplicate copy of the user's profile. During the synchronization process, a temporary profile is created in the user's context. This process debits the user's quota. If a user's disk quotas are set too low, roaming profile synchronization might fail.

If possible, use profile quotas to manage disk space and apply disk quotas *only* if additional control is required.

Do not use Offline Folders on roaming user profile shared folders

To prevent synchronization problems, make sure that you turn off Offline Folders for shared folders where roaming user profiles are stored. If you do not turn off Offline Folders for a user's profile, you might experience synchronization problems because both Offline Folders and Roaming User Profiles try to synchronize the files in a user's profile. This synchronization conflict does not affect using Offline Folders with redirected files, such as **My Documents**.

Group Policy Recommendations for Roaming User Profiles

Use the following guidelines for setting Group Policy for roaming user profiles to help to ensure optimum functionality.

Reducing disk space use, profile size, and logon processing

To save disk space, you can use the **Delete cached copies of roaming profiles** policy setting to specify that locally cached versions of roaming user profiles be deleted when the user logs off. This setting is in the **Computer Configuration\Administrative Templates\System\User Profiles** node of the Group Policy Object Editor snap-in.

To manage the user profile size, use the **Limit profile size** policy setting. This setting is in the **User Configuration\Administrative Templates\System\User Profiles** node of the Group Policy Object Editor snap-in. You can set the maximum size of the roaming user profile and determine the system's response when the limit is reached. When you set this policy, the Proquota.exe program is enabled. This program alerts users when their user profile exceeds a predefined limit, and it prevents users from logging off until the size of the profile files is reduced.

To reduce both profile size and logon processing time, you can use the **Exclude directories in roaming profile** setting to designate certain folders to exclude from the user's profile. This setting is in the **User Configuration\Administrative Templates\System\User Profiles** node of the Group Policy Object Editor.

Turning off the fast logon enhancement

With the fast logon enhancement in Windows XP, when users change from a local to a roaming profile, two logons on each computer are required for profile changes to be registered. This is because the user always logs on with cached credentials. Therefore, it takes one logon for the network to detect that the user has become a roaming user and a second logon to apply the new settings.

To ensure the best user experience, enable the **Always wait for the network at computer startup and logon** policy setting. This setting is in the **Computer Configuration\Administrative Templates\System\Logon** node of the Group Policy Object Editor.

Limiting use of Group Policy loopback processing if you use roaming profiles

The **User Group Policy loopback processing mode** policy setting is an advanced option that is intended to keep the desktop configuration the same regardless of who logs on. This option is appropriate for use in certain closely managed environments, such as classrooms, public kiosks, reception areas, servers, and terminal servers. When you enable the loopback processing policy setting in a GPO, you can configure user-based policy settings within that GPO, and those settings are applied regardless of which user logs on to the computer, meaning that those settings override individual user settings. When you use the **User Group Policy loopback processing mode** policy setting, you must ensure that both the computer and user portions of the GPO are enabled. The **User Group Policy loopback processing mode** policy setting is available in the **Computer Configuration\Administrative Templates\System\Group Policy** node of the Group Policy Object Editor.

By default, the user's Group Policy objects determine which user settings apply. When you enable this policy setting, you also specify either the *Replace mode* or the *Merge mode*, which determines the policies that are applied.

Replace mode The user settings that are defined in the computer's Group Policy objects replace the user settings that are typically applied to the user.

Merge mode The user settings that are defined in the computer's Group Policy objects and the user settings that are typically applied to the user are combined. If the settings conflict, the user settings in the computer's Group Policy objects take precedence over the user's policy settings.

If you disable or do not configure the **User Group Policy loopback processing mode** setting, the user's Group Policy objects determine which user settings apply.



Caution

Use caution when using loopback policy processing and roaming profiles, especially if roaming users use two or more computers that run different versions of the Windows operating system, including Windows Server 2003, Windows 2000, Windows XP, and Windows NT 4.0. You might see some settings persist in the registry because applications can store policy settings in the HKEY_CURRENT_USER\Software\Policies subkey regardless of the operating system version. Windows NT 4.0 also stores some Internet Explorer policy settings in the HKEY_CURRENT_USER\Software\Microsoft\windows\currentversion\explorer\policies subkey, and those settings persist in the registry. Windows Server 2003, Windows 2000, and Windows XP clear these registry subkeys each time before re-applying the current Group Policy object settings. However, Windows NT 4.0 does *not* clear the registry subkeys, which causes some settings to persist if you roam from a computer that runs Windows Server 2003, Windows 2000, or Windows XP.

Additional Policy Settings That Are Related to User Profiles

Tables 7.5 and 7.6 list additional Group Policy settings that you can set for user profiles. These policy settings are available in **Group Policy Object Editor** in the **User Configuration\Administrative Templates\System\User Profiles** and **Computer Configuration\Administrative Templates\System\User Profiles** respectively. For more information about the policy settings, click the **Explain** tab on each policy's **Properties** page.

Table 7.5 Policy Settings for User Profiles: User Configuration

Policy Setting	Description
Connect home directory to root of the share	Restores the definitions of the %HOMESHARE% and %HOMEPATH% environment variables to those that are used in Windows NT 4.0 and earlier. If you enable this setting, the system uses the Windows NT 4.0 definitions. Along with %HOMEDRIVE%, these variables define the home directory of a user profile. The home directory is a persistent mapping of a drive letter on the local computer to a local or remote directory.

Table 7.6 Policy Settings for User Profiles: Computer Configuration

Policy Setting	Description
Delete cached copies of roaming profiles	Determines whether the system saves a copy of a user's roaming profile on the local computer's hard disk drive when the user logs off. This policy and the related policies in this folder define a strategy for managing user profiles that reside on remote servers. Specifically, these policies indicate to the system how to respond when a remote profile is slow to load.
Slow network connection timeout for user profiles	Defines a slow connection for roaming user profiles. If the server on which the user's roaming user profile resides takes longer to respond than the thresholds that are set by this policy permit, the system considers the connection to the profile to be slow. This policy and related policies in this folder together determine how the system responds when roaming user profiles are slow to load.
Add the Administrators security group to the roaming user profile share	<p>This setting adds the Administrator security group to the roaming user profile shared folder. After an administrator has configured a user's roaming profile, the profile is created at the user's next login at the location that is specified by the administrator.</p> <p>For Windows 2000 and Windows XP operating systems, the default file permissions for the newly generated profile are full control, or read and write access for the user, and no file access for the administrators group. By configuring this setting, you can alter this behavior. If you enable this setting, the administrator group is given full control to the user's profile folder.</p>
Prevent roaming profile changes from propagating to the server	This policy determines if the changes a user makes to their roaming profile are merged with the server copy of their profile. If this policy is set, at logon users receive their roaming profile, but any changes users make to their profile are not merged to the users' roaming profile at logoff.
Only allow local profiles	<p>This setting determines if roaming user profiles are available on a particular computer. By default, when roaming profile users log on to a computer, their roaming profile is copied to the local computer. If they have previously logged on to this computer, the roaming profile is merged with the local profile. When the users log off this computer, the local copy of their profile, including any changes they have made, is merged with the server copy of their profile.</p> <p>If you enable this setting, the following occurs on the affected computer: At first logon, the user receives a new local profile, rather than the roaming profile. At logoff, changes are saved to the local profile. All subsequent logons use the local profile.</p>
Prompt user when slow link is detected	<p>Notifies users when their roaming profiles are slow to load, letting a user decide whether to use a local copy or to wait for the roaming user profile.</p> <p>If you disable this policy or do not configure it, the system does not notify the user when a roaming user profile is slow to load. The system loads the local copy of the profile. If you enable the Wait for remote user profile policy, the system loads the remote copy without prompting the user.</p>
Maximum retries to unload and update user profile	Applies to Windows 2000 only. This setting determines how many times the system tries to unload and update the registry portion of a user profile.

	When the number of trials that is specified by this policy is exhausted, the system stops trying. As a result, the user profile might not be current, and local and roaming user profiles might not match.
Do not detect slow network connections	Disables the slow link detection feature. <i>Slow link detection</i> measures the speed of the connection between a user's computer and the remote server that stores the roaming user profile. When the system detects a slow link, the related policies in this folder tell the system how to respond.
Wait for remote user profile	Directs the system to wait for the remote copy of the roaming user profile to load even when loading is slow. The system waits for the remote copy when the user is notified about a slow connection but does not respond within the time allowed.
Timeout for dialog boxes	Determines how long the system waits for a user response before it uses a default value. The default value is used when the user does not respond to messages. Use this setting to override the system's default value of 30 seconds.

Security Recommendations for Roaming User Profiles Shared Folders

You need to ensure that access permissions are set appropriately on shared folders that contain user profile folders and to secure the servers in which the users' data is stored. To provide enhanced security, host the roaming profile shared folders on servers running Windows 2000 or later, use NTFS on the volumes containing the users' data, and grant share access permissions as follows.

Granting profile share permissions

A common error in user profiles is permissions that are incorrectly set. To ensure that permissions are set correctly, use the following guidelines:

- When you create the shared folders for roaming user profiles, limit access to the folder to only users who need access.
- Because a roaming profile contains personal information, such as the user's documents and EFS certificates, it is important to ensure that roaming user profiles are secure. Here are some ways you can enhance the security of roaming user profiles:
 - Restrict the shared folder to only users who need access. Create a security group for users who have profiles on a particular shared folder, and then limit access to only those users.
 - When you create the shared folder, hide the folder by putting a dollar sign (\$) after the share name. This hides the folder from casual browsers and hides the folder in **My Network Places**.
 - Unless you need special permissions on the profile folder, do not create profile folders in advance for the user. Instead, allow the system to create them.

- Assign users the minimum permissions that are required as described in Tables 7.7, 7.8, and 7.9. These tables list the required NTFS and share level server message block (SMB) permissions for roaming user profile shares and folders.

Table 7.7 NTFS Permissions for Roaming Profile Parent Folder

User Account	Minimum Permissions Required
Creator Owner	Full Control, Subfolders and Files Only
Administrator	None
Security group of users needing to put data on share	List Folder/Read Data, Create Folders/Append Data - This Folder Only
Everyone	No permissions
Local System	Full Control, This Folder, Subfolders and Files

Table 7.8 Share level (SMB) Permissions for Roaming Profile Share

User Account	Default Permissions	Minimum Permissions Required
Everyone	Read only	No permissions
Security group of users needing to put data on share	N/A	Full Control

Table 7.9 NTFS Permissions for Each User's Roaming Profile Folder

User Account	Default Permissions	Minimum Permissions Required
%Username%	Full Control, Owner of Folder	Full Control, Owner of Folder
Local System	Full Control	Full Control
Administrators	No Permissions*	No Permissions
Everyone	No Permissions	No Permissions

* No permissions is the default unless the **Add the Administrator security group to the roaming user profile share** policy setting is set, in which case the Administrators group has full control. (The **Add the Administrator security group to the roaming user profile share** policy setting requires Windows 2000 Service Pack 2 or later).

Hosting profile shares on servers running Windows 2000 or Windows Server 2003

A user's roaming profile contains personal information that is copied to and from the client computer and the server that hosts the roaming profile; therefore, it is important to ensure that the data is protected as it travels over the network.

The major potential threats to the privacy and integrity of a user's data come from malicious users intercepting and tampering with data as it passes over the network, or the server hosting the user's data.

Several features of Windows 2000 and Windows Server 2003 can help to secure a user's data:

- **Kerberos.** Standard on all versions of Windows 2000–based servers, Kerberos ensures the highest level of security to network resources. While NTLM authenticates the client only, Kerberos authenticates the server and the client. When NTLM is used, the client does not detect whether the server is valid. This is particularly important if the client exchanges personal files with the server, as is the case with roaming profiles. Kerberos provides better security than NTLM and is not available on Windows NT 4.0 or earlier operating systems.
- **IP Security Protocol (IPSec).** IPSec provides network-level authentication, data integrity, and encryption to ensure that roamed data is safe from the following:
 - Data modification while en route
 - Interception, viewing, or copying
 - Access by unauthenticated parties

For more information about IPSec, see the *Networking Guide* of the *Windows Server 2003 Resource Kit* “(or see the Networking Guide” on the Web at <http://www.microsoft.com/reskit>).

- **Server Message Block Signing.** The SMB authentication protocol supports message authentication. This prevents active message and “man-in-the-middle” attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server. To use SMB signing, you must either enable it or require it on both the SMB Service client and the SMB Service server.

**Note**

SMB signing imposes a performance penalty even though it does not consume any more network bandwidth; it does use more CPU cycles on the client and server.

Using the NTFS File System for Volumes Containing User Data

For the most secure configuration, always configure servers that host roaming profiles to use NTFS. Unlike a file allocation table (FAT), NTFS supports discretionary access control lists (DACLs) and system access control lists (SACLs) which determine who can perform operations on a file and what events trigger logging of actions performed on a file.

Configuring Roaming User Profiles

Before you create a roaming user profile, you need to create each user account. Then, log on to a server as an administrator to create a network share to store the roaming user profiles, designate the groups of users to receive the roaming user profiles, and grant all users Full Control permissions.

Use the following procedures when you create and manage roaming user profiles.

Creating Roaming User Profiles

To perform the following procedure, you must be a member of the Account Operators group, Domain Admins group, or the Enterprise Admins group in Active Directory, or you must have

been delegated the appropriate authority. For enhanced security, consider using the **Runas** command to perform this procedure.

► **To create a roaming user profile**

1. Open **Active Directory Users and Computers**.
2. Click the domain and the OU where the user account resides.
3. Right-click the user account for which to set a roaming profile, and then click **Properties**.
4. Click the **Profile** tab, and then type the profile path information in **Profile path**. (Use the full path in each user account. For example, type `\\Server\ShareName\UserName`.)

Another way to populate the profile path is to use an Active Directory® Service Interfaces (ADSI) script. ADSI provides a single set of interfaces for managing resources on the network. You can use ADSI in combination with Microsoft® Visual Basic® Scripting Edition (VBScript) or JScript scripts to manage Active Directory resources such as users and services.

For information about ADSI and ADSI scripts, see the Microsoft Platform SDK link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Changing User Profile Type from Local to Roaming

Typically, a large organization has many users with local profiles. For ease of management, you might want to change many of the local profiles to roaming profiles. Moving user's data and settings from the workstation to a server reduces the user's dependence on the workstation's availability, simplifies user data management, and allows centralized account management.

► **To create a roaming user profile for a user that has a local profile**

5. Open **Active Directory Users and Computers**.
6. Click the domain and the OU where the user account resides.
7. Right-click the appropriate user account for which to set a roaming profile, and then click **Properties**.
1. Click the **Profile** tab, and type the profile path information in **Profile path** (for example, type `\\Server\ShareName\UserName`).



Note

To change a user's local profile to a roaming profile for a user who uses multiple computers simultaneously, the user must log off last from the computer that has the profile that the user wants to use.

Disabling Roaming User Profiles on Certain Computers

You can prevent computers from receiving roaming profiles by enabling the **Only allow local user profiles** policy setting, which blocks roaming profiles from being used on a computer. By default, when roaming profile users log on to a computer, the user's roaming profile is copied to the local computer. If the user has previously logged on to this computer, the roaming profile is merged with the local profile. Similarly, when the user logs off from this computer, the local

copy of the profile, including any changes the user made, is merged with the server copy of the profile.

If you enable the **Only allow local user profiles** policy setting, the following occurs on the affected computer: When the user first logs on, the user receives a new local profile instead of the roaming profile. At logoff, changes are saved to the local profile. All subsequent logons use the local profile.

If you enable both the **Prevent Roaming Profile changes from propagating to the server** setting and the **Only allow local user profiles** setting, roaming profiles are disabled for that computer. These policy settings are in the **Computer Configuration\Administrative Templates\System\User Profiles** node.

Creating Accounts That Possess roaming user profiles

You can save time and reduce the chances for error by scripting many repetitive tasks, such as creating user accounts. A script to automate the creation of user profiles for roaming user might look something like the sample script Listing 7.1, which shows a script for creating user accounts that have roaming profiles.

Listing 7.1 Creating User Accounts That Have Roaming User Profiles

```

1  set Args = Wscript.Arguments
2  ouName = Args(0)
3  usrName = Args(1)
4  RUProot = Args(2)
5
6  RUPpath = RUProot & "\" & usrName
7
8  'Get the domain
9  Set dse = GetObject("LDAP://RootDSE")
10 Set domain = GetObject( "LDAP://" & dse.Get("defaultNamingContext"))
11
12 set ou = domain.GetObject("organizationalUnit", "OU=" & ouName )
13
14 wscript.echo "Creating user in " & ou.Name
15
16 set usr = ou.Create("user", "cn=" & usrName )
17 usr.Put "samAccountName", usrName
18 usr.Put "userPrincipalName", usrName
19 usr.Put "Profilepath", RUPpath
20
21 usr.SetInfo
22
23 wscript.echo " User " & usrName & " was created successfully in " & ou
24 & "with a RUP Path of: " & RUPpath

```

Every Windows Server 2003 user has a profile. If the operating system does not have a profile to apply to the user when the user logs on, a new local profile is created for the user, based on the defaults in place. Windows Server 2003 applies a generic user profile format by default.

Configuring a Default Profile

You can create a default profile to ensure that all users within a domain receive an identical profile the first time they log on. This option simplifies administrative control over the users' desktops and settings.

To create a default user profile, you must be logged on as Administrator or a member of the Administrators group. Create a default profile for all new user accounts in a domain. Include any domain-specific customizations that you want in the profile. To create subsequent profiles, you can create a new user account as a template.

Before creating a new user account to use as a new user's profile template, perform the following tasks:

1. Log on to the domain as the new user, and then customize the desktop if appropriate.
2. Optionally, install and configure any applications to be shared by user accounts made from this template.
3. Log off, and then log on as the administrator.

For more information about creating a new user account, see "Create a new user account" in Help and Support Center for Windows Server 2003.

► To configure a new user account to use as a new user's profile template

1. After you create a new user account template, in **Control Panel**, click **System**.
2. On the **Advanced** tab, under **User Profiles**, click **Settings**.
3. Under **Profiles stored on this computer**, select the user that you created in step 1, and then click **Copy To**.
4. To create the default user profile for the domain, type the path to NETLOGON\Default User on the domain controller.
5. In the **Copy To** dialog box, under **Permitted to use**, click **Change**.
6. In the **Select User or Group** dialog box, enter the object name to select, and then type: **Everyone**.

Troubleshooting: Creating a Log File for User Profiles

User profiles log events in the Application event log. To aid in troubleshooting, administrators can also create detailed log files by using the following procedure.



Caution

Do not edit the registry unless you have no alternative. The registry editor, regedit.exe, bypasses standard safeguards, allowing settings that can damage your system, or even require you to reinstall Windows. If you edit the registry, make sure to back it up first and see the Registry Reference on the *Windows Server 2003 Deployment Kit* companion CD or at <http://www.microsoft.com/reskit>.

► To create a detailed log file for user profiles

1. In the **Run** dialog box, type **regedit**, and then click **OK**.
2. Locate the following subkey:
HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon.
3. Create a new entry named **UserEnvDebugLevel** of data type **REG_DWORD**, and set its value to 0x30002.

The log file is stored in this location: %windir%\Debug\Usermode\Userenv.log.

Implementing Folder Redirection

Folder Redirection is simple to configure and manage. While Folder Redirection reduces the disk space that is required on the client, it requires network shares to accommodate the redirected folders. By combining Folder Redirection and roaming user profiles, you can decrease logon and logoff times for roaming and mobile users. Besides the improved availability and backup benefits of having the data on the network, users also have performance gains with low-speed network connections and subsequent logon sessions.

By using Folder Redirection in conjunction with roaming user profiles, you can also provide fast computer replacement. If a user's computer needs to be replaced, the data that a user requires can quickly be re-established on a replacement computer.

Recommendations for Folder Redirection

To get the best performance from Folder Redirection, it is recommended that you: create the root share on the server and let the system create the users' folders, synchronize files at logoff when you use Folder Redirection with Offline Files, and use the following guidelines for redirecting **My Documents**, and setting options for Offline Files.

Letting the system create folders for each user

For optimal performance of the Folder Redirection feature, it is strongly recommended that you create *only* the root share on the server, and then let the system create the folders for each user. If you must create the folders for users, ensure that you correctly assign permissions. For more information about assigning permissions see "Security Recommendations for Folder Redirection" later in this chapter.



Important

If you must create folders for users, make sure that you set the correct permissions. Then, clear the **Grant exclusive rights to** check box on the **Settings** tab of the **Folder Redirection Properties** page. If you do not clear this check box, Folder Redirection first checks preexisting folders to determine if the user is the owner. If the administrator previously created the folder, the check fails, and redirection is cancelled. Folder Redirection logs an event in the Application event log indicating that redirection failed and that the new directories for the redirected folder cannot be created due to not being able to assign a security ID as the owner of the folder (Event ID 101).

Accepting the default settings for Folder Redirection

If you are storing roaming user profiles on the server where you have enabled Offline Files, Folder Redirection ensures that Offline Files are set to synchronize when the user logs on and logs off.

For Windows 2000 and earlier clients, if you are using Offline Files in conjunction with Folder Redirection and roaming user profiles, it is recommended that you leave the default setting of synchronizing Offline Files at logoff enabled to ensure best performance of these features. This is because if a shared folder is unavailable, Offline Files considers the entire server to be unavailable until the offline cache is manually synchronized. Roaming profiles are *not* synchronized with the server while Offline Files treats the server as being unavailable. For clients that run Windows XP or later, whether the default synchronization setting is selected or not, roaming profiles continue to roam even if Offline Files has marked the server as being offline.

Using offline files settings

Using offline files settings on a server share where the user data is stored is especially useful for users of portable computers. It is recommended that you use Folder Redirection in conjunction with Offline Files. Table 7.10 lists the recommendations for Offline Files.

Table 7.10 Recommendations for Configuration of Offline Files

Redirected Folder	Recommended Offline Files Settings
My Documents	All files and programs that users open from the share will be automatically available offline <i>or</i> Only the files and programs that users specify will be available offline (if you want users to manually designate files and folders to be available offline).
My Pictures	All files and programs that users open from the shared folder will be automatically available offline <i>or</i> Only the files and programs that users specify will be available offline.
Application Data	All files and programs that users open from the share will be automatically available offline.
Desktop	All files and programs that users open from the share will be automatically available offline if the desktop is read only.
Start Menu	All files and programs that users open from the share will be automatically available offline.

Redirecting My Documents

The following suggestions for redirecting the My Documents folder are appropriate for most deployments and can provide a faster and simpler deployment.

- Redirect My Documents to a network share.
- Allow Folder Redirection to create folders for you. When setting redirection policy for a group, use the path to the share, such as `\\server\share`. Folder Redirection then appends the user name and the folder name when the policy is applied.

- Allow Folder Redirection to perform all the moving of folders and files when you select a folder for redirection or change the target network share to which you redirect the folder. The Folder Redirection client not only moves files to the appropriate network share, but it also sets proper folder security and renames entries in the Offline Files cache database so that they continue to link to the correct target folders and files. Any files pinned by the user in the Offline File Cache stay pinned.
- Combine Folder Redirection with Offline Files to provide the user access to **My Documents**, even when the user's workstation is temporarily disconnected from the network. This is particularly useful for people who use portable computers. For more information, see "Make a file or folder available offline" in Help and Support Center for Windows Server 2003.
- Include redirected folders, particularly **My Documents**, in routine server backups. Performing backups of user data that is located on network shares is simpler and more reliable because it requires no action on the part of the user or interaction with the workstation.
- Use Group Policy to set profile quotas and disk quotas to establish limits on the disk space that is used by users' data and settings.
- Redirect user-specific data from the hard disk that holds the operating system files. This data can be redirected to a different hard disk on the user's local computer or to a network share. This simplifies system maintenance by separating system files from user files.
- Centralize storage on large shares to reduce workstation hardware and maintenance costs. Pooling disk space more than offsets the cost of increasing server disk capacity.
- Do not use the **Redirect to home folder** policy setting unless you have already deployed home folders in your organization.
- Leave the **My Pictures** folder located in the **My Documents** folder.

When you redirect the **My Documents**, the Recycle Bin size for **My Documents** defaults to a percentage of the size of the server partition where the redirected **My Documents** resides. You can manually change this size in 1 percent increments. Because a Recycle Bin can grow large, encourage users to empty their Recycle Bins periodically.

**Note**

You can grant users exclusive rights to their redirected folders. Select the **Grant the user exclusive rights to My Documents** check box under the **Settings** tab in each folder's **Properties** dialog box to grant full control over the folder to the user and the local system only.

Redirect folders to home folders

Typically, it is recommended that you do *not* redirect to a home directory unless you have already deployed home directories in your organization. However, if you have home directories and want to transition your users to use **My Documents** while maintaining compatibility with the home directory environment, you can redirect a user's **My Documents** folder to the user's home folder. The **Redirect to home folder** policy setting is intended *only* for organizations in which home folders are already in place. Redirect only the **My Documents** folder to the home folder.

For this type of redirection, the client computer must run one of the following operating systems: Windows XP Professional, Microsoft® Windows XP, 64-Bit Edition, or Windows Server 2003. This redirection option does not work for clients that run Windows NT, Windows 2000, or Microsoft® Windows® XP Home Edition.

When a folder is redirected to the home folder, security and ownership are not checked, and permissions are not changed. Folder Redirection behaves as though the administrator has set directory security correctly. This relaxed security is the reason that redirection to the home folder is not recommended if the home folder structure is not already in place, and you have not updated your configuration.

Typically, folder redirection fails if a user is not the owner of the folder to which the **My Documents** folder is redirected. Because redirection to the home folder is intended for an earlier environment, Folder Redirection does not check for proper folder ownership. Instead, ownership check is left to the administrator.

Users must have the home folder property set correctly on their user object in Active Directory. The client computer gets the path for the user's home folder from the user object in Active Directory when the user logs on. User accounts that have redirected folders must have this path set correctly, or Folder Redirection fails.

For more information about creating home folders for profiles, see "Add a home folder to a profile" in Help and Support Center for Windows Server 2003.

Combining Folder Redirection with Offline Files

The Offline Files technology applies to network shares or mapped drives that contain documents or data that a user might want to use offline. Folder Redirection and Offline Files are functionally independent but complementary in operation.

Folder Redirection provides user access to redirected folders that have been relocated to network shares. Offline Files provides the user with access to any specified folder or file when the network share is unavailable, or offline.

Redirecting the Start Menu folder

Folder Redirection of the **Start** Menu folder is available in Windows XP, Windows XP 64-Bit Edition, or Windows Server 2003 operating systems. **Start** Menu redirection is treated differently from other redirected folders in that the contents of the user's **Start** Menu are not copied to the redirected location. It is assumed that a redirected **Start** Menu has been previously created by an administrator and that all users share the same **Start** Menu. As a best practice for Windows XP-based computers, do *not* use Folder Redirection to redirect the **Start** Menu folder; instead, use Group Policy to control what appears on the **Start** Menu.

Redirecting application data and use of Outlook

If a user redirects the **Application Data** folder and runs multiple instances of the Microsoft Outlook messaging and collaboration client on different computers, including an instance of Microsoft® Outlook 2000, mail opening performance is delayed. Outlook 2000 continually keeps the Outcmd.dat file open. (This file stores information about toolbar customizations that users make in Outlook.) When another instance of Outlook tries to access Outcmd.dat, it is unable to access it because Outlook 2000 has locked the file. The second copy of Outlook repeatedly tries to access Outcmd.dat, causing a delay when the user tries to open or reply to messages.

**Note**

Outlook 2002, included in Microsoft® Office XP, does *not* hold the Outcmd.dat file open. This behavior occurs *only* when Outlook 2000 is running on one of the computers.

Encrypted file system considerations

Folder Redirection has implications for encrypted files that are located in redirected folders.

- Files redirected to a server can be encrypted by Encrypting File System (EFS) *only* if an administrator has designated the remote server as *trusted for delegation*. Administrators can establish a service or computer as trusted for delegation to allow that service or computer to complete delegated authentication, receive a ticket for the user who makes the request, and then access information for that user.
- Encrypted files are decrypted before being transmitted over the network. File encryption only protects the files while they reside on the disk.
- The Offline Files cache cannot be encrypted on Windows 2000 Professional.

For more information about delegating trust and enabling delegated authentication, see “Designing an Authentication Strategy” in *Designing and Deploying Directory and Security Services* of this kit.

Group Policy Recommendations for Folder Redirection

Use the following Group Policy guidelines to ensure that offline files are fully synchronized and available when users work offline, and to specify the behavior of redirected folders and their contents when a Group Policy object no longer applies.

Enabling the Synchronize all offline files before logging off Policy Setting

Always enable the **Synchronize all offline files before logging off** policy setting to ensure that offline files are fully synchronized and that all the files in the users’ redirected folder are available when users work offline. If this setting is not enabled, the operating system only performs a quick synchronization, and only recently used files are cached. The **Synchronize all offline files before logging off** policy setting is available in the **Computer Configuration\Administrative Templates\Network\Offline Files** node of the Group Policy Object Editor.

Removing Group Policy

It is important to consider the behavior of your Folder Redirection policy settings when Group Policy is removed. To specify Group Policy removal options, use the selected folder’s **Properties** page and select the **Settings** tab. You can access this page under **User Configuration\Windows Settings\Folder Redirection** of the Group Policy Object Editor by right-clicking a folder (for example, **Application Data**), clicking **Properties**, and then selecting the **Settings** tab to specify the policy removal options to use.

Table 7.11 indicates what happens to redirected folders and their contents when a Group Policy object no longer applies.

Table 7.11 Summary of Folder Properties Page Settings for Redirected Folders

Setting: Move the contents of special folder to the new location option	Policy Removal Option	Result of Removal
Enabled	Redirect the folder back to the user profile location when policy is removed	<ul style="list-style-type: none"> The special folder returns to its user profile location. The folder contents are copied back to the user profile location. The contents are not deleted from the redirected location. The user can continue to access the contents, but only on the local computer.
Disabled	Redirect the folder back to the user profile location when policy is removed	<ul style="list-style-type: none"> The special folder returns to its user profile location. <p>Note: In this case, the folder contents are not copied or moved to the user profile location. As a result, the user can no longer see the contents.</p>
Either Enabled or Disabled	Leave the folder in the new location when policy is removed	<ul style="list-style-type: none"> The special folder remains at its redirected location. The contents remain at the redirected location. The user continues to have access to the contents at the redirected folder.

**Important**

Changing the redirection option to **No Administrative policy specified** does not redirect the folder to the local profile, this option means that Folder Redirection is not configured — *if a folder was previously redirected it continues to be redirected to the previous location*. If you want to return the folder to the local user profile, use the **Redirect the folder back to the user profile location when policy is removed** option.

Security Recommendations for Folder Redirection

Use the following guidelines when you create the shares for redirected folders to ensure you set access permissions appropriately, and to help provide the most secure configuration.

Restricting access to the share

Redirected folders contain personal information such as documents and EFS certificates so it is important to protect this data.

- Create a security group for users who have redirected folders on a particular share and limit access only to those users
- Create a hidden share by putting a dollar sign (\$) after the share name. The share is not visible in the network neighborhood.
- Grant users the minimum permissions that are required to access the data.

Assigning permissions for root folder, shares, and user's redirected folder

Tables 7.12, 7.13, and 7.14 show the permissions for the folder redirection root, share, and the users' redirected folders.

Table 7.12 NTFS Permissions for Folder Redirection Root Folder

User Account	Minimum Permissions Required
Creator Owner	Full Control, Subfolders and Files Only
Administrator	None
Security group of users that need to put data on share	List Folder/Read Data, Create Folders/Append Data - This Folder Only
Everyone	No Permissions
Local System	Full Control, This Folder, Subfolders and Files

Table 7.13 Share level (SMB) Permissions for Folder Redirection Share

User Account	Default Permissions	Minimum permissions required
Everyone	Full Control	No permissions
Security group of users that need to put data on share.	N A	Full Control

Table 7.14 NTFS Permissions for Users' Redirected Folders

User Account	Default Permissions	Minimum permissions required
%Username%	Full Control, Owner of Folder	Full Control, Owner of Folder
Local System	Full Control	Full Control
Administrators	No permissions	No permissions
Everyone	No permissions	No permissions

Host redirected file shares on servers running Windows 2000 or Windows Server 2003

To provide the best protection as data is transmitted over the network, ensure that you set up the redirected folders shares on servers running Windows 2000 and later. The Kerberos, IPSec, and SMB signing security features of Windows 2000 and Windows Server 2003 help protect the users' data.

Using the NTFS file system for user data volumes

Always configure the servers hosting redirected files to use NTFS to provide the most secure configuration.

Do not rely on EFS to encrypt users' files when transmitted over the network

When you use EFS to encrypt files on a remote server, the data is encrypted *only* while it is stored on the disk, not when it is transmitted over the network. The exceptions to this are when your system includes IPSec or Web Distributed Authoring and Versioning (WebDAV). IPSec encrypts data while it is transported over a TCP/IP network. If the file is encrypted before being copied or moved to a WebDAV folder on a server, it remains encrypted during the transmission and while it is stored on the server.

Encrypting the Offline Files cache

While access control lists (ACLs) protect the Offline Files cache on NTFS partitions by default, encrypting the cache enhances security on a local computer. By default, the cache on the local computer is *not* encrypted, so any encrypted files that are cached from the network are not encrypted on the local computer. This might pose a security risk in some environments.

When you enable encryption, all files in the Offline Files cache are encrypted, including existing files and any files that you add later. The cached copy on the local computer is affected, but the associated network copy is not.

You can encrypt the cache in one of two ways:

- By using Group Policy to enable the **Encrypt the offline files cache** policy setting. This setting is in the **Computer Configuration\Administrative Templates\Network\Offline Files** node in the Group Policy Object Editor snap-in.
- Manually, by clicking **Folder Options** on the **Tools** menu in **Windows Explorer**. Click the **Offline Files** tab, and then select the **Encrypt offline files to secure data** check box.



Note

Encryption of the Offline File cache is only available in Windows XP and Windows Server 2003; it is *not* possible to encrypt the cache on Windows 2000-based computers.

For information about encrypting the Offline Files cache for Windows XP, see the How to Encrypt Offline Files link on the Web resources page at <http://www.microsoft.com/windows/reskits/webresources>. For information about encrypting files for Windows 2000, see the Encrypting File System for Windows 2000 link on the Web resources page.

Configuring Folder Redirection

Use the Group Policy Object Editor snap-in to redirect special folders to network locations.

The primary tasks that pertain to configuring Folder Redirection include:

- Creating or selecting a GPO for Folder Redirection.

- Selecting **Basic** or **Advanced** Folder Redirection options. **Advanced** redirection allows you to apply the redirection to users that belong in a specified security group.
- Identifying the target folder location. You can redirect folders to any of the following locations:
 - The root of a network file share
 - A folder on a network share
 - A local folder
 - A home directory (only applicable if you have existing home directories in your environment)
- Setting permissions for root folders and users' folders.

**Note**

If you allow Folder Redirection to create the redirected folders on a specified network, the folders that are created in this way have proper permissions assigned to them. If you create the folders manually, you must make sure that permissions are properly assigned.

Redirecting Special Folders

In most cases, you should redirect special folders to the root directory instead of to a specific location because this appends the correct paths for you, including %username%.

► To redirect special folders to the root directory

1. Open a GPO that is linked to the site, domain, or OU that contains the users whose special folders you want to redirect.
2. In the console tree, under **User Configuration\Windows Settings\Folder Redirection**, double-click **Folder Redirection** to display the special folder that you want to redirect.
3. Right-click the special folder that you want to redirect (such as **Desktop** or **My Documents**), and then click **Properties**.
4. Click the **Target** tab, and then in the **Settings** box, select **Basic - Redirect everyone's folder to the same location**.
5. Under **Target folder location**, select **Create a folder for each user under the root path**.
6. In the **Root Path** box, type a Universal Naming Convention (UNC) path, such as `\\servername\sharename`, and then click **OK**.
7. In the **Properties** dialog box for the special folder, click **OK**.

The user name and folder name are appended to the UNC path automatically.

► To redirect special folders to a specific path

1. Open a GPO that is linked to the site, domain, or OU that contains the users whose special folders you want to redirect.

2. In the console tree, under User Configuration\Windows Settings\Folder Redirection, double-click Folder Redirection to display the special folder that you want to redirect.
3. Right-click the special folder that you want to redirect, and then click **Properties**.
4. In the **Setting** box on the **Target** tab, select **Basic - Redirect everyone's folder to the same location**.
5. Under **Target folder location**, select **Redirect to the following location**. In the **Root Path** box, type an UNC path, such as \\server\share, or type a locally valid path, such as C:\somefolder, and then click **OK**.

If necessary, you can return redirected folders to their original default locations by using the following procedure.

► **To redirect special folders to the local profile location**

1. Open a GPO that is linked to the site, domain, or OU that contains the users whose special folders you want to redirect.
2. In the console tree, double-click Folder Redirection to display the special folder that you want to redirect.
3. Right-click the special folder that you want to redirect (such as Desktop or My Documents), and then click **Properties**.
4. In the **Setting** box on the **Target** tab, select **Basic - Redirect everyone's folder to the same location**.
5. Under **Target folder location**, select **Redirect to the local user profile location**, and then click **OK**.

Redirecting to the home directory

It is recommended that you do *not* redirect to a home directory unless you have already deployed home directories in your organization. However, if you have already deployed home directories and you want to maintain compatibility with your existing home directory environment, you can redirect My Documents to the home directory.

► **To redirect My Documents to the home directory**

1. Open a GPO that is linked to the site, domain, or OU that contains the users whose My Documents folders you want to redirect.
2. In the console tree, double-click Folder Redirection to display My Documents.
3. Right-click My Documents, and then click **Properties**.
4. In the **Setting** box, on the **Target** tab, select **Basic - Redirect everyone's folder to the same location**.
5. Under **Target folder location**, select **Redirect to the user's home directory**, and then click **OK**.

**Note**

Domain administrators have full control over the users' My Documents folder when you redirect My Documents to the home directory. This is the case even if you select the **Grant the user exclusive rights to My Documents** option on the **Settings** tab in the **My Documents Properties** dialog box.

Redirecting special folders based on membership in security groups

You can redirect special folders for use by members of security groups to the root directory, a specific path, the local profile directory, or to the home directory.

► To redirect special folders to the root directory based on security group membership

1. Open the GPO that contains the users whose special folders you want to redirect.
2. In the console tree, double-click Folder Redirection to display the special folder that you want to redirect (for example, Desktop or My Documents), right-click the special folder, and then click **Properties**.
3. On the **Target** tab, in the **Setting** box, select **Advanced - Specify locations for various user groups**, and then click **Add**.
4. In the **Specify Group and Location** dialog box, under **Security Group Membership**, type the name of the security group, or click **Browse** to search for it.
5. Under **Target Folder Location**, select **Create a folder for each user under the root path**.
6. In **Root Path**, type the UNC path to use for redirection (for example, \\servername\sharename), and then click **OK**.
7. In the special folder's Properties dialog box, click **OK**.

For more information about Folder Redirection, in Help and Support Center for Windows Server 2003, on the toolbar, click the **Index** button, in **Type in the keyword to find**, type **folder redirection**, and then double-click the topic that you want in the index list.

Troubleshooting: Creating a Log File for Folder Redirection

Folder Redirection logs events in the Application Event Viewer log. To aid troubleshooting, administrators can also create detailed log files for Folder Redirection.

**Caution**

Do not edit the registry unless you have no alternative. The registry editor, regedit.exe, bypasses standard safeguards, allowing settings that can damage your system, or even require you to reinstall Windows. If you edit the registry, make sure to back it up first and see the Registry Reference on the *Windows Server 2003 Deployment Kit* companion CD or at <http://www.microsoft.com/reskit>.

► To enable logging for Folder Redirection

1. In the **Run** dialog box, type **regedit**, and then click **OK**.

2. Locate the following subkey:
HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Diagnostics.
3. Create a new entry called FdeployDebugLevel of data type Reg_DWORD, and set its value to 0x0f.

The log file is created in %windir%\Debug\Usermode\Fdeploy.log.

Implementing Offline Files and Synchronization

By deploying the Offline Files technology, you allow network users to access files that are stored on network shares, even when the client computer is not connected to the network. A mobile user that accesses the share while disconnected from the network can still browse, read, and edit files because the files are cached on the client computer. You can initiate synchronization manually or set Synchronization Manager to control the synchronization of offline files with the network.

The Offline Files technology provides either a *full* or *quick* synchronization. A full synchronization ensures that the most current version of every network file that has been made available offline is available. A quick synchronization is much faster than a full synchronization, and it ensures that a complete version of each cached file is available. The quick synchronization does not ensure that each cached file is the most current version of every network file that has been made available offline. The quick synchronization ensures that each file in the offline cache is a complete. For more information about Offline Files, file synchronization, and managing user data and settings, see the *Distributed Services Guide* of the *Windows Server 2003 Resource Kit* (or see the Distributed Services Guide on the Web at <http://www.microsoft.com/reskit>).

Recommendations for Using Offline Files

By using Offline Files, you can manage user data more efficiently while enhancing users' access to their files and folders. When combined with Folder Redirection, Offline Files improves availability; when combined with Synchronization, Offline Files increases the reliability of content.

Files and Folders You Can Make Available Offline

You can make available for offline use any shared files or folders on a Microsoft network. You can make files available offline from any computer that supports Server Message Block-based file and printer sharing, including Microsoft® Windows® 95, Microsoft® Windows® 98, Windows NT 4.0, and the Windows Server 2003 family.

You can set up shared folders so that every network file the user opens in that shared folder is available offline. Alternatively, you can specify which network files are made available offline. Table 7.15 shows typical Offline Files caching settings for each redirected folder.

**Note**

If you make a shortcut to a file available offline, that file is made available offline. However, if you make a shortcut to a *folder* available offline, the contents of that folder are not available offline.

Table 7.15 Offline Files Settings

Special Folder	Offline File Settings
My Documents	All files and programs that users open from the share will be automatically available offline or Only the files and programs that users specify will be available offline to allow users to designate files and folders for offline use.
My Pictures	All files and programs that users open from the share will be automatically available offline or Only the files and programs that users specify will be available offline so users can designate files and folders for offline use.
Application data	All files and programs that users open from the share will be automatically available offline.
Desktop	All files and programs that users open from the share will be automatically available offline if the desktop is Read Only.
Start Menu	All files and programs that users open from the share will be automatically available offline.

Offline Files Caching Options

In the Windows Server 2003 family, Offline Files is, by default, not enabled. When enabled, the following three types of Offline Files caching are available:

- **Only the files that users specify will be available offline** (previously called **Manual Caching for Documents**). Provides offline access to only those files on a network share that have been manually selected. Manual caching for documents is the default option when you set up a shared folder to use offline.
- **All files and programs that users open from the share will be automatically available offline** (previously called **Automatic Caching for Documents** and **Automatic Caching for Programs**). Selecting this option makes every file that someone opens from your shared folder available offline. However, only those files that have been opened are available offline.
- **Files or programs from the share will not be available offline**. Selecting this option prevents users from storing files offline.

In Windows XP and Windows Server 2003, the default behavior is to cache all redirected folders automatically. Even if you specify manual caching for a redirected folder, the folder is still subject to automatic caching. To disable this default behavior, enable the **Do not automatically make redirected folders available offline** policy setting, available in **User Configuration\Administrative Templates\Network\Offline Files**. If you enable this policy setting, the users must manually select the files to be made available offline.

Combining Offline Files with EFS

When you use Offline Files, you can specify that offline files are encrypted. If you choose to encrypt offline files, only the files on your local computer are encrypted. The files on the network are not encrypted, nor are the files encrypted as they traverse the network.

The **Encrypt offline files to secure data** setting is disabled under the following conditions:

- You are not an administrator on the computer.
- The local drive is not NTFS or does not support encryption.
- A system administrator has implemented an encryption policy for Offline Caching.
- The Offline Files technology is not available in Windows XP Home Edition.
- In the Windows Server 2003 family, Offline Caching is not enabled by default.

Deploying Offline Files on Terminal Services Clients

Multi-user Terminal Services disables Offline Files on computers that run Windows Server 2003. Terminal Services on Windows XP Professional is always single user, but Terminal Services on servers is multi-user by default. To use Terminal Services and Offline Files together on servers, set the value of the **AllowMultipleTSSessions** registry entry to 0. This entry is found in the following registry subkey:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon



Caution

Do not edit the registry unless you have no alternative. The registry editor bypasses standard safeguards, allowing settings that can damage your system, or even require you to reinstall Windows. If you must edit the registry, back it up first and see the Registry Reference on the *Windows Server 2003 Deployment Kit* companion CD or at <http://www.microsoft.com/reskit>.

Offline Files and Synchronization Manager

The copies of offline files that are stored in the Offline Files data store are kept up to date by Synchronization Manager. The Synchronization Manager tool is invoked when users with roaming user profiles log on, log off, or access selected files or folders.

Caching Offline Files

Offline Files notifies users when the status of the network connection changes. A message notifies users when they are offline, and the users can continue working with the files. When they work offline, users can still browse network drives and shared folders that are set up for Offline Files. A red X appears over any disconnected network drives that are not currently available. For more information about their network connection status, users can click the **Offline Files** icon in the notification area.

When the network connection is restored, any changes the user made while working offline are updated to the network. If other users have made changes to the same file, options are offered to

the users for resolving the version conflict. For more information, see “Handling file conflicts” in Help and Support Center for Windows Server 2003.

Forcing Synchronization

A user who is concerned about losing network connectivity can force synchronization to ensure that local copies of network files are current.

You can use Synchronization Manager to perform periodic synchronizations to ensure that users’ offline files are kept current.



Note

To keep offline files current with minimal interruption to users, schedule offline files to be synchronized whenever users’ computers are idle.

Synchronizing Offline Files

If you configure Offline Files, you need to decide the appropriate time to synchronize offline files. You also have a choice of two methods, full or quick. For a *full synchronization*, enable the **Synchronize all offline files before logging off** policy setting. Disabling this policy causes a *quick synchronization* to be performed when the user logs off.

A full synchronization ensures that you have the most current versions of every network file that has been made available offline. A quick synchronization ensures that you have complete versions of all your offline files, even if they are not the most current versions.

In Windows Server 2003, the **Synchronize all offline files when logging on** policy setting mirrors the **Synchronize all offline files before logging off** policy setting. Both policy settings are available in both User Configuration and Computer Configuration under **Administrative Templates\Network\Offline Files**. For more information, see the **Explain** tab on the **Properties** page of each policy.

By default, the Offline Files feature is not enabled in the Windows Server 2003 family because any Terminal Services mode that allows multiple, concurrent user logon sessions is not compatible with Offline Files. Offline Files is enabled by default in Windows XP Professional and Windows 2000 Professional.

To maximize the benefits of Offline Files, the Synchronization Manager service frequently synchronizes server and client copies of any offline file. However, synchronization makes demands on file system and network resources.

Configuring Group Policy for Offline Files

Tables 7.16 and 7.17 list the Offline Files policy settings that administrators can use. The settings are available in **User Configuration\Administrative Templates\Network\Offline Files** and in **Computer Configuration\Administrative Templates\Network\Offline Files** in the Group Policy Object Editor snap-in. For more information about policy settings, see the **Explain** tab on the **Properties** page of each policy.

**Note**

Most of the policy settings exist in both the User Configuration and the Computer Configuration nodes.

Table 7.16 User Configuration Policy Settings for Offline Files

Policy Setting	Description
Prohibit user configuration of Offline Files¹	<p>Prevents users from enabling, disabling, or changing the configuration of Offline Files.</p> <p>This setting removes the Offline Files tab from the Folder Options dialog box. It also removes the Settings item from the Offline Files shortcut menu and disables the Settings button on the Offline Files Status dialog box. As a result, users cannot view or change the options on the Offline Files tab or in the Offline Files dialog box.</p> <p>This is a comprehensive policy setting that locks down the configuration that you establish by using other settings in this folder.</p>
Synchronize all Offline Files when logging on¹	<p>Determines whether offline files are fully synchronized when users log on.</p> <p>This setting also disables the Synchronize all offline files before logging on option on the Offline Files tab. This prevents users from changing the option while a setting controls it.</p>
Synchronize all Offline Files before logging off¹	<p>Determines whether offline files are fully synchronized when users log off.</p> <p>This setting also disables the Synchronize all offline files before logging off option on the Offline Files tab. This prevents users from trying to change the option while a setting controls it.</p>
Synchronize Offline Files before suspend	<p>Determines whether offline files are synchronized before a computer is suspended.</p> <p>If you enable this setting, offline files are synchronized whenever the computer is suspended. Setting the synchronization action to Quick ensures only that all files in the cache are complete. Setting the synchronization action to Full ensures that all cached files and folders are up to date with the most current version.</p> <p>If the computer is suspended by closing the display on a portable computer, synchronization is not performed. If multiple users are logged on to the computer at the time the computer is suspended, synchronization is not performed.</p>
Action on server disconnect¹	<p>Determines whether network files remain available if the computer is suddenly disconnected from the server that is hosting the files.</p> <p>This setting also disables the When a network connection is lost option on the Offline Files tab, which prevents users from trying to change the option while a setting controls it.</p> <p>Also, see the Non-default server disconnect actions policy setting in this table.</p>
Non-default server disconnect actions²	<p>Determines how computers respond when they are disconnected from particular offline file servers.</p> <p>This setting overrides the default response, a user-specified response, and the response that is specified in the Action on server disconnect policy setting. This setting does not prevent users from setting custom actions on the Offline Files tab. However, users cannot change any custom actions that were established by means</p>

	of this setting.
Remove 'Make Available Offline'¹	Prevents users from making network files and folders available offline. This setting removes the Make Available Offline option from the File menu and from all shortcut menus in Windows Explorer. As a result, users cannot designate files to be saved on their computer for offline use. However, this setting does not prevent the system from saving local copies of files that reside on network shares that are designated for automatic caching.
Prevent use of Offline Files folder¹	Disables the Offline Files folder. This setting disables the View Files button on the Offline Files tab. As a result, users cannot use the Offline Files folder to view or open copies of network files that are stored on their computer. Also, they cannot use the folder to view characteristics of offline files, such as their server status, type, or location. This setting does not prevent users from working offline or from saving local copies of files available offline. Also, it does not prevent users from using other programs, such as Windows Explorer, to view their offline files.
Administratively assigned offline files³	Lists network files and folders that are always available for offline use. This setting makes the specified files and folders available offline to users of the computer.
Turn off reminder balloons¹	Hides or displays reminder balloons, and prevents users from changing the setting. Reminder balloons appear above the Offline Files icon in the notification area to notify users when they have lost connection to a networked file and are working on a local copy of the file. Users can then decide how to proceed.
Reminder balloon frequency¹	Determines how often reminder balloon updates appear. Reminder balloons appear when the user's connection to a network file is lost or reconnected, and they are updated periodically. By default, the first reminder for an event is displayed for 30 seconds. Then, updates appear every 60 minutes and are displayed for 15 seconds. You can use this setting to change the interval between updates.
Initial reminder balloon lifetime¹	Determines how long the first reminder balloon for a network status change is displayed.
Reminder balloon lifetime¹	Determines how long updated reminder balloons are displayed.
Event logging level¹	Determines which events the Offline Files feature records in the event log. Offline Files records events in the Application event log when it detects errors. By default, Offline Files records an event only when the offline files storage cache is corrupted. However, you can use this setting to specify additional events that you want Offline Files to record.
Prohibit 'Make Available Offline' for these files and folders⁴	Prohibits specific network files and folders from being made available for offline use. This setting does not prevent files from being automatically cached if the network share is configured for automatic caching. It only affects the availability of the Make Available Offline menu option in the user interface.

	If the Remove 'Make Available Offline' setting is enabled, this setting has no effect.
Do not automatically make redirected folders available offline	<p>By default, makes all redirected shell folders, such as My Documents, Desktop, Start Menu, and Application Data, are available offline.</p> <p>This setting allows you to change this behavior so that redirected shell folders are not automatically available for offline use. However, users can still choose to make files and folders available offline.</p> <p>Do not enable this setting unless you are certain that users do not need access to all of their redirected files in the event that the network or the server holding the redirected files becomes unavailable.</p> <p>This setting does not prevent files from being automatically cached if the network share is configured for automatic caching, nor does it affect the availability of the Make Available Offline menu option in the user interface.</p>

¹ This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

² This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured for a particular server, the setting in Computer Configuration takes precedence over the setting in User Configuration. Both Computer and User configurations take precedence over a user's setting.

³ This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the settings are combined and all specified files are available for offline use.

⁴ This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the settings are combined, and the specified files are *not* available for offline use.



Note

Most Offline Files policy settings in the User Configuration node, listed in Table 7.16, also appear in the Computer Configuration node. Table 7.17 lists *only* those settings that are unique to the Computer Configuration node. For more information about the settings, open the **Explain** tab on the **Properties** page of each policy.

Table 7.17 Computer Configuration Policy Settings for Offline Files

Policy Setting	Description
Allow or disallow use of the Offline Files feature	<p>Determines whether the Offline Files feature is enabled.</p> <p>This setting also disables the Enable Offline Files option on the Offline Files tab. This prevents users from changing the option while a setting controls it.</p> <p>By default, Offline Files is enabled in Windows 2000 Professional and is disabled in Windows 2000 Server.</p>
Default cache size	<p>Limits the percentage of the computer's disk space that can be used to store automatically cached offline files.</p> <p>This setting also disables the Amount of disk space to use for temporary offline files option on the Offline Files tab. This prevents users from changing the option while a setting controls it.</p> <p>Automatic caching can be set on any network share. When a user opens a file on the</p>

	<p>share, the system automatically stores a copy of the file on the user's computer. This setting does not limit the disk space available for files that users make available offline manually.</p>
Files not cached	<p>Lists types of files that cannot be used offline.</p> <p>This setting lets you exclude certain types of files from automatic and manual caching for offline use. The system does not cache files of the type that is specified in this setting even when they reside on a network share that is configured for automatic caching. Also, if users try to make a file of this type available offline, the operation will fail and the following message is displayed in the Synchronization Manager Progress dialog box: "Files of this type cannot be made available offline."</p>
At logoff, delete local copy of users offline files	<p>Deletes local copies of the user's offline files when the user logs off.</p> <p>This setting specifies that automatically and manually cached offline files are retained only while the user is logged on to the computer. When the user logs off, the system deletes all local copies of offline files.</p> <p>Caution: Files are not synchronized before they are deleted. Any changes to local files since the last synchronization are lost.</p>
Subfolders always available offline	<p>Makes subfolders available offline whenever their parent folder is made available offline.</p> <p>This setting automatically extends the Make available offline policy setting to all new and existing subfolders of a folder. Users do not have the option of excluding subfolders.</p>
Encrypt the Offline Files cache	<p>Determines whether offline files are encrypted.</p> <p>Offline files reside on a user's hard disk, not the network, and they are stored in a local cache on the computer. Encrypting this cache enhances security on a local computer. If the cache on the local computer is not encrypted, any encrypted files cached from the network will not be encrypted on the local computer. This might pose a security risk in some environments.</p> <p>By default, this cache is protected on NTFS partitions by ACLs.</p>
Configure Slow link speed	<p>Configures the threshold value at which Offline Files considers a network connection to be slow.</p> <p>Any network speed below this value is considered to be slow.</p>

Security Recommendations for Shared Resources



Note

When you create a new shared resource, offline access is permitted by default; this means that secure shared resources can be stored offline on potentially unsecured computers. You must ensure that you set appropriate permissions by using share permissions or access control on the NTFS file system.

Assigning permissions to groups, not to user accounts

Assigning permissions to groups simplifies the management of shared resources because you can then add users to or remove them from the groups without having to reassign permissions. To deny all access to a shared resource, deny the Full Control permission.

Assigning the most restrictive permissions that still allow users to perform required tasks

For example, if users only need to read information in a folder, and they will never delete, create, or change files, assign the Read permission.

Centralizing the administration of shared resources

On computers running Windows XP Professional that are connected to a domain, allow access to shared resources by using domain user accounts, instead of by using local user accounts. This centralizes the administration of share permissions.

Denying permissions

Avoid explicitly denying permissions to a shared resource unless you want to override specific permissions that are already assigned.

Using NTFS file system permissions or access control shared resources

Use NTFS file system permissions and access control if users log on locally to access shared resources (such as Terminal Services). Share permissions apply only to users who access shared resources over the network; they do not apply to users who log on locally.

Organizing resources for objects with similar security requirements

Organize resources so that objects with the same security requirements are located in the same folder. For example, if users require Read permissions for several application folders, store the application folders in the same parent folder. Then, share the parent folder, instead of each individual application folder. If you need to change the location of an application, you might need to reinstall it.

Limiting membership in Administrators group

To enable administrators to manage application software and to control user rights, limit membership in the Administrators group, and assign Full Control permissions to that group.

Creating a strong password

To keep drives secure, make sure that you use a strong password for all accounts. A strong password has the following characteristics:

- Is at least seven characters long.

- Does not contain your user name, real name, or company name.
- Does not contain a complete dictionary word.
- Is significantly different from previous passwords and does not contain incremental numbers or letters — such as Password1, Password2, Password3 or PasswordA, PasswordB, and so on.
- Contains characters from each of the following four groups: upper case letters, lower case letters, numerals, and symbols. An example of a strong password is J*p2leO4>F.

You can use Group Policy to enforce password complexity requirements. You can configure the **Password must meet complexity requirements** security setting by selecting the appropriate GPO and expanding the console tree: **Computer Configuration\Windows Settings\Security Settings\Account Policies>Password Policy**. For more information about password policy, see “Apply or modify password policy” in Help and Support Center for Windows Server 2003.

Using a firewall

To protect shared resources from unauthorized Internet access, use a firewall. For more information about making shared resources more secure, see “Securing shared resources” in Help and Support Center for Windows Server 2003.

Configuring Offline Files

Offline Files technology applies to any mapped or mounted drive that contains documents that users might want to use offline. You set up and configure Offline Files independently of the Folder Redirection snap-in extension. The default state (Enabled or Disabled) of the Offline Files feature depends on the operating system version that you are running, as indicated in Table 7.18.

Table 7.18 Default State of the Offline Files Feature

Operating System Version	Offline Files State
Windows 2000 Professional	Enabled
Windows XP Professional	Enabled
Windows 2000 Server	Disabled
Windows Server 2003 family products	Disabled. The Offline Files feature is not compatible with Terminal Services.

Enabling the Offline Files Feature for Windows Server 2003 Computers

By enabling the Offline Files features in Windows Server 2003, you can set up a computer to use Offline Files or make file or folder available offline.

► To enable Offline Files on a server running Windows Server 2003

1. Right-click **My Computer**, and then click **Properties**.
2. In the **System Properties** dialog box, click the **Remote** tab.

3. Under **Remote Desktop**, clear the **Allow users to connect remotely to this computer** check box, and then click **OK**.

► **To set up a computer to use Offline Files**

1. In **My Computer**, on the **Tools** menu, click **Folder Options**.
2. On the **Offline Files** tab, select **Enable Offline Files**.

-Or-

To do a quick synchronization, clear the **Synchronize all offline files before logging off** check box.

After you set up a computer to use Offline Files, select the files and folders that you want to make available offline.

► **To make a file or folder available offline**

1. Open **My Computer**, and then right-click the shared file or folder that you want to make available offline.
2. On the **File** menu, click **Make available offline**.
3. Follow the instructions in the Offline Files Wizard.

Configuring Offline Settings

Offline Files stores a version of the shared resources on the client computer in the file system *cache*, a reserved portion of disk space, which the client computer can access even when it is disconnected from the network. You can set caching options for each shared resource to specify which files or programs will be available offline.

► **To configure offline settings for shared files or folders**

1. Open Computer Management.
2. In the console tree, navigate to System Tools, Shared Folders, and then Shares.
3. In the details pane, right-click the shared file or folder for which you want to configure offline settings, and then click **Properties**.
4. On the **General** tab, click **Offline Settings**.
5. In the **Offline Settings** dialog box, select one of the following options, and then click **OK**.
 - **Only the files and programs that users specify will be available offline.** (The default option that gives users control over which files are available offline.)
 - **All files and programs that users open from the share will be automatically available offline.** (Allows all the files that users open from the shared folder to be automatically available offline.) If you select the **Optimized for performance** check box, all programs are automatically cached so that they can run locally. This option is especially useful for file servers that host applications because it reduces network traffic and improves server scalability.
 - **Files or programs from the share will not be available offline.** This option prevents users from storing files offline.

**Note**

When you use the option for automatic caching of all files and programs, be sure to restrict permissions on the files and programs that are contained in the shared folder to read-only access.

After you configure Offline Files, configure Synchronization Manager to periodically ensure that the Offline Files cache has a complete and correct copy of every file that is designated for offline use.

On client computers running Windows XP Professional or Windows Server 2003, redirected folders are automatically added to Offline Files storage. In Windows 2000, you can enable this feature, but it is not enabled by default.

You can make individual files from a shared network folder or an entire shared network folder available offline. If you create a shortcut to a *file* that is available offline, the file is also available offline. If you create a shortcut to a *folder* that is available offline, the contents of that folder are *not* available offline.

For a procedure to store offline files and folders in a network share, see “Set client-side caching for a File Share resource” in Help and Support Center for Windows Server 2003.

**Tip**

Use the Group Policy setting **Administratively assigned offline files** to set multiple folders at the same time for offline use.

Configuring Synchronization Manager

Synchronization Manager maintains offline files that are stored in the Offline Files cache on the user’s workstation. You can configure Synchronization Manager to initiate Offline File synchronization in response to one or more of the following situations:

- When the user logs on or off the computer
- At specific intervals while the computer is idle
- At scheduled times

Synchronizing Files and Folders

Use the **Synchronization Manager** wizard to specify the items to synchronize and to define options for the synchronization process.

**To open Synchronization Manager**

- In the **Run** dialog box, type **mobsync**, and then click **OK**.

**To synchronize offline items**

1. Open Synchronization Manager.

2. In the **Select the check box for any items you want to synchronize** box, under **Name**, select the check box for each offline item that you want to synchronize, and then click **Synchronize**.
- **To synchronize individual files, folders, or Web pages**
1. Open Windows Explorer, My Computer, or Internet Explorer.
 2. Select the item that you want to synchronize, and then on the **Tools** menu, click **Synchronize**.
- **To synchronize offline items when you log on to or log off from a computer**
1. Open Synchronization Manager, click **Setup**, and then click the **Logon/Logoff** tab.
 2. In **When I am using this network connection**, click the network connection that you want to use.
 3. In **Synchronize the following checked items**, select the check box for the offline items that you want to synchronize.
 4. Under **Automatically synchronize the selected items**, do one of the following:
 - To synchronize items when you log on to your computer, select the **When I log on to my computer** check box.
 - To synchronize items when you log off of your computer, select the **When I log off my computer** check box.
 - To request permission before synchronizing your offline items, select the **Ask me before synchronizing the items** check box.
- **To schedule offline items to synchronize**
1. Open **Synchronization Manager**, click **Setup**, and then click the **Scheduled** tab.
 2. Click **Add** to start the Scheduled Synchronization Wizard, and then follow the instructions in the wizard.
- **To synchronize offline items while your computer is idle**
1. Open Synchronization Manager, click **Setup**, and then click the **On Idle** tab.
 2. Click the network connection that you want to use.
 3. In **When I am using this network connection**, click the network connection that you want to use.
 4. In **Synchronize the following checked items**, select the check box for the offline items that you want to synchronize.
 5. Select the **Synchronize the selected items while my computer is idle** check box.

Assigning Profile and Disk Quotas

Typically, the disk space that users need varies, depending on users' roles.

Consolidating user disk space on network shares is more efficient and cost-effective than providing large amounts of storage at each workstation. However, you need to manage the shares. Profile and disk quotas can assist you in monitoring and managing network shares.

Profile Quotas and Local Drives

Profile quotas do not restrict redirected folders because they are not stored in the user's profile. If you want to reduce disk space requirements of workstations, do not save profiles locally. To establish quotas, apply profile quotas instead of disk quotas to local disk drives.

Combining Redirection of My Documents with Roaming User Profiles

If you combine Folder Redirection of the **My Documents** folders with Roaming User Profiles, do *not* apply disk quotas to the volume in which roaming profiles are stored. Instead, use a profile quota to manage the size of the profile, and use a disk quota to manage the size of the **My Documents** and **My Pictures** folders.



Note

If you are combining Folder Redirection of the **My Documents** folder and roaming user profiles, it is recommended that you do *not* use disk quotas on the profile folders. The operating system and applications write items to the user profile folder on the user's behalf. This includes items such as Custom.dic and Favorites.

Limiting Profile Size

To manage the profile quota size, use the **Limit profile size** policy setting in the Group Policy Object Editor snap-in. This policy sets the maximum size of each roaming user profile and determines the system's response when a roaming user profile reaches the maximum size. The **Limit profile size** policy setting is available in the **User Configuration\Administrative Templates\System\User Profiles** node of the Group Policy Object Editor.

Removing Cached Copies of Roaming Profile to Minimize Disk Space Usage

If disk size on a multi-user computer is a concern (for example, a public computer that numerous users use), you can use the **Delete cached copies of roaming profiles** policy, which removes cached versions of the profile when a user logs off. The **Delete cached copies of roaming profiles** policy setting is available in the **Computer Configuration\Administrative Templates\System\User Profiles** node of the Group Policy Object Editor.

Setting Quotas on User Profiles

To manage the size of a user profile, you can set a maximum profile quota or remove local copies of a user's roaming profile from the workstation when a user logs off.

► To set a maximum profile quota

1. Open the Group Policy Object Editor snap-in.
2. In **User Configuration\Administrative Templates\System\User Profiles**, double-click the **Limit profile size** policy setting.
3. In the **Limit profile size Properties** page, click **Enable**, specify the options you want to use, and then click **OK**.

- **To remove local copies of a user's roaming profile from the workstation when a user logs off**
1. Open Group Policy Object Editor.
 2. In the **Computer Configuration\Administrative Templates\System\User Profiles** folder, double-click the Delete cached copies of roaming profiles policy setting.
 3. Click **Enable**, and then click **OK**.

Deleting cached profiles when the user logs off adds time to the logon process; however, it is recommended for workstations in locations that are not secure. User profile data needs to be treated as confidential. Ideally, such data is only retained on computers that are physically secure.

Over-Allocating Disk Space

Some tasks, such as moving large folders within a disk volume, require a user to temporarily allocate a large amount of disk space. This temporary space is more readily available if it is pulled from a large pool of space. Therefore, you need to allocate more space for each user than they need for long-term storage.

Determination of the total quantity of shared disk space to be made available to users is influenced by historical requirements, planned deployments of new servers and user accounts, and your hardware purchasing budget. Typically, the median disk usage is much higher than the average disk usage due to the varying allocations of disk space in a large group of users.

Requirements for Managing Disk Quotas

Disk quotas track and control disk space usage for user data that is stored on the network. You can set disk quotas by using Group Policy. When disk quotas are enabled in Group Policy, the settings affect all NTFS volumes on all computers running Windows 2000, Windows XP Professional, or Windows Server 2003 to which the GPO applies. Alternatively, you can manually set disk quotas on individual servers.

To administer disk quotas, you must be a member of the Administrators group. You can set quotas on local volumes, network volumes, and removable drives that are formatted with NTFS. The network volumes must be shared from the volume's root directory, and removable drives must be shared.

Recommendations for Using Disk Quotas

Apply disk quota limits according to the actual disk space your users need.

1. Try to estimate how much disk space various types of users will require and then categorize users according to their disk space requirements (for example, users who work with art programs might require a large amount of disk space).
2. Next, structure your disk volumes by those categories, and then use disk quotas to limit the amount of disk space allowed for the users on each volume.
3. Also, consider metadata. Each file stored on the volume can use up to 64 kilobytes (KB) of NTFS metadata that is not applied to a user's quota limit. To avoid running out of disk space, ensure that you provide sufficient disk space to accommodate this metadata.

Setting default quota limits

Set moderately restrictive default limits for all user accounts, and then modify the limits to allow more disk space to users who work with large files. You might want to increase disk quota limits for a few user accounts rather than to force some users to work with a quota limit that does not meet their needs. User policy settings occupy at least 2 MB of disk space, so you should set the default limits for all user accounts above 2 MB.

Setting limits that permit growth in disk space use

Set the quota level to allow for increasing use of disk space. Increase quota when necessary as a percentage of the current quota setting.

Group Policy for Disk Quotas

Table 7.19 lists the Group Policy settings for disk quotas. These settings are available in the **Computer Configuration\Administrative Templates\System\Disk Quotas** node.

Table 7.19 Disk Quota Policy Settings in Disk Quotas

Policy Setting	Description
Enable disk quotas	Enables and disables disk quota management on all NTFS volumes of the computer and prevents users from changing the setting.
Enforce disk quota limit	Determines whether disk quota limits are enforced and prevents users from changing the setting.
Default quota limit and warning level	Specifies the default disk quota limit and warning level for new users of the volume.
Log event when quota limit exceeded	Determines whether the system records an event in the local Application log when users reach their disk quota limit on a volume, and prevents users from changing the logging setting.
Log event when quota warning level exceeded	Determines whether the system records an event in the Application log when users reach their disk quota warning level on a volume.
Apply policy to removable media	Extends the disk quota policies in this folder to NTFS file system volumes on removable media.

Group Policy for Disk Quota Processing

Administrators can use Group Policy to specify how often disk quotas are applied. The **Disk quota policy processing** policy setting is available under **Computer Configuration\Administrative Templates\System\Group Policy**. This policy applies to all policy settings that use the disk quota component of Group Policy, such as those in **Computer Configuration\Administrative Templates\System\Disk Quotas**.

The **Quota policy processing** policy setting includes the following options:

- **Allow processing across a slow network connection.** Updates the policies even when the update is being transmitted across a slow link. Updates across slow connections can cause significant delays.

- **Process even if the Group Policy objects have not changed.** Updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a setting in case a user has changed it.
- **Do not apply during periodic background processing.** Prevents the system from updating affected policies in the background while the computer is in use.



Caution

Background updates can disrupt the user, cause a program to stop or operate abnormally, and, in rare cases, damage data.

Administrators and users with rights to create computer objects can circumvent quota restrictions. This is because they can create any number of computer accounts, each with the default quota limit.

Configuring Disk Quotas on NTFS Volumes

To enable disk quotas, you must be a member of the Administrators group on the local computer, or you must have been delegated the appropriate authority.

► To enable disk quotas

1. Open My Computer, right-click the disk volume for which you want to enable disk quotas, and then click **Properties**.
2. On the **Quota** tab, click the **Enable quota management** check box.
3. Specify the quota limits, thresholds, and event logging options that you want to use, and then click **OK**.

Table 7.20 shows the available options for disk quotas.

Table 7.20 Quota Management Options

Option	Description
Deny disk space to users exceeding quota limit	Users who exceed their quota limit receive an “insufficient disk space” error message from Windows and cannot write additional data to the volume without first deleting or moving some existing files from it. Individual programs determine their own error handling for this condition. To the program, it appears that the volume is full. If you clear this check box, users can exceed their quota limit. Enabling quotas and not limiting disk space use are useful when you do not want to deny users access to a volume but want to track disk space use on a per-user basis. You can also specify whether to log an event when users exceed either their quota warning level or their quota limit.
Limit disk space to	Enter the amount of disk space that new users of the volume are allowed to use and the amount of disk space that must be used before an event is written to the system log. Administrators can view these events in Event Viewer. You can use decimal values (for example, 20.5). For the disk space and warning levels, select the appropriate units from the drop-down list (for example, KB, MB, or GB).

Log event when a user exceeds their quota limit	If quotas are enabled, an event is written to the system log on the local computer whenever users exceed their quota limit. Administrators can view these events in Event Viewer and filter for disk event types. By default, quota events are written hourly to the system log on the local computer. You can change the interval at which quota events are written to the system log on the local computer using the fsutil behavior command. Fsutil is a command-line tool that you can use to perform tasks related to FAT and NTFS file systems.
Log event when a user exceeds their warning level	If quotas are enabled, an event is written to the system log on the local computer whenever users exceed their quota warning level. Administrators can view these events in Event Viewer, filtering for disk event types. By default, quota events are written hourly to the system log on the local computer. You can change the interval at which quota events are written to the system log on the local computer by using the Fsutil behavior command.

For more information about using disk quotas, see “Disk quotas” in Help and Support Center for Windows Server 2003. For more information about the command-line tool **Fsutil**, in Help and Support Center for Windows Server 2003, click **Tools**, and then click **Command-line reference A–Z**.

Desktop Strategies for Computers Running Windows 2000 and Windows XP Without Active Directory

If you have computers running Windows 2000 Professional and Windows XP Professional in a domain that does *not* include Active Directory, you can manage desktops locally by implementing the following features:

Roaming User and Logon Scripts When using either a Windows NT 4.0 domain or Active Directory, both roaming user profiles and logon scripts are configured on the user object.

Folder Redirection You can redirect special folders to alternate locations, either to a local or network location by modifying the values of the registry entries in the following registry subkey: `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders`

Redirecting folders by using logon scripts

Group Policy is the recommended method for redirecting user’s folders. You can also achieve similar results by using logon scripts to set values of the registry entries in the subkey **User Shell Folders**. This approach provides functionality that is similar to Folder Redirection.

In Windows NT 4.0 environments, you can use System Policy to set the appropriate values. However, when you use System Policy to set values, the registry settings persist. And you do not get the advantages of using Group Policy to set paths such as automatic moving of files when the path changes.

Internet Explorer Maintenance Instead of using Group Policy to control Internet Explorer

settings, administrators can use the Internet Explorer Administration Kit (IEAK) to apply settings to Internet Explorer clients using auto-configuration packages. For more information about IEAK, see the Microsoft Internet Explorer Administration Kit (IEAK) link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

System Policy (for registry-based policy) Domain-based Group Policy processing requires that the User and Computer objects be located in Active Directory. If the User or Computer objects are located in a Windows NT 4.0 domain, then Windows NT 4.0 System Policy is processed for whichever of these objects is located in that domain — this could be the Computer or User object, or both. System Policy is defined as the policy mechanism that is used natively in Windows NT 4.0; it is a set of registry settings that together define the computer resources that are available to a group of users or an individual.

Local Group Policy object You can set settings in the local Group Policy object (LGPO) for any computer, whether or not it participates in an Active Directory domain. Although System Policy scales more easily to a large number of clients, the LGPO can be useful if you only need to apply certain settings to a small number of Windows XP Professional or Windows 2000–based clients in a Windows NT 4.0 or other domain.

The LGPO is located at `\systemroot\System32\GroupPolicy`. Not all Group Policy extensions are available for the local GPO. Each Group Policy extension snap-in queries the Group Policy engine to get the GPO type, and then determines whether the GPO is to be displayed. To set the LGPO, use the Group Policy snap-in focused on the local computer. You can use a LGPO to set policy for these Group Policy extensions only: scripts, security settings, Administrative Templates, and Internet Explorer maintenance; you cannot set policy for Software Installation, Folder Redirection, and Remote Installation Services.

Additional Resources

These resources contain additional information and tools related to this chapter.

Related Information

- The *Distributed Services Guide* of the *Windows Server 2003 Resource Kit* (or see the Distributed Services Guide on the Web at <http://www.microsoft.com/reskit>) for more information about Group Policy and advanced Group Policy
- “Deploying a Managed Software Environment” in this book
- The User Data and Settings Management link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources> for information about managing user data and settings for Windows XP in a Windows 2000 environment
- The Group Policy Management Console link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources> for information about Group Policy management tools

Related Tools

- Diruse.exe

You can use the command-line tool **Diruse.exe** to gather disk usage information for compressed files and folders in NTFS volumes, such as how much disk space each folder uses in a directory tree on a disk volume. For more information about **Diruse.exe**, in Help and Support Center for Windows Server 2003, click **Tools**, and then click **Windows Support Tools**.

- **Fsutil**

You can use the **Fsutil** command-line tool to perform many tasks related to file allocation table (FAT) and NTFS file systems, such as managing reparse points, managing sparse files, or dismounting a volume. **Fsutil** is a powerful tool that should only be used by administrators who have a thorough knowledge of Windows XP or the Windows Server 2003 family of operating systems. For more information about **Fsutil**, in Help and Support Center for Windows Server 2003, click **Tools**, and then click **Command-line reference A–Z**

Related Job Aids

- “Worksheet A.39 Determining User Requirements” (DMEUSE_39.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.39 Determining User Requirements” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.40 Determining Server Disk Space Requirements” (DMEUSE_40.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.40 Determining Server Disk Space Requirements” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.41 Considerations for Mobile Users” (DMEUSE_41.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.41 Considerations for Mobile Users” on the Web at <http://www.microsoft.com/reskit>).

Related Help Topics

For best results in identifying Help topics by title, in Help and Support Center, under the **Search** box, click **Set search options**. Under **Help Topics**, select the **Search in title only** check box.

- “Using roaming user profiles” in Help and Support Center for Windows Server 2003 for more information about implementing roaming user profiles
- Group Policy topics in Help and Support Center for Windows Server 2003 for more information about working with GPOs
- “Create a new user account” in Help and Support Center for Windows Server 2003
- “Make a file or folder available offline” in Help and Support Center for Windows Server 2003
- “Add a home folder to a profile” in Help and Support Center for Windows Server 2003
- “Handling file conflicts” in Help and Support Center for Windows Server 2003
- “Apply or modify password policy” in Help and Support Center for Windows Server 2003
- “Securing shared resources” in Help and Support Center for Windows Server 2003 for more information about making shared resources more secure

- “Set client-side caching for a File Share resource” in Help and Support Center for Windows Server 2003 for a procedure to store offline files and folders in a network share
- “Disk quotas” in Help and Support Center for Windows Server 2003

Deploying a Managed Software Environment

8

By using Group Policy–based software management, you can centrally deploy, install, and manage applications throughout an organization. From a central location, you can also perform routine maintenance tasks such as upgrading, patching, and removing applications without going to individual workstations. You can also configure Software Restriction Policies to prevent users from running unknown or dangerous programs.

In This Chapter

Deploying a Managed Software Environment Overview	344
Preparing Applications for Deployment	352
Deploying Applications in a Managed Environment	370
Migrating Applications to a Managed Environment	400
Patching, Upgrading, and Removing Applications.....	405
Troubleshooting Software Deployment.....	420
Additional Resources.....	426

Related Information

- For information about deploying Group Policy and using the new Group Policy Management console (GPMC) MMC snap-in, see “Designing a Group Policy Infrastructure” in this book.
- For more information about managing Group Policy–based software deployment, see the *Distributed Services Guide* of the *Microsoft® Windows® Server 2003 Resource Kit* (or see the *Distributed Services Guide* on the Web at <http://www.microsoft.com/reskit>).

Deploying a Managed Software Environment Overview

Software administrators face ongoing challenges for deploying and maintaining software. They must ensure that users have reliable access to necessary software while preventing unknown or dangerous software from being installed or run. Users can, for example, unintentionally turn a desktop environment into an administrator's nightmare by deleting files and programs or by downloading unsupported software from the Internet or from removable media such as a CD-ROM.

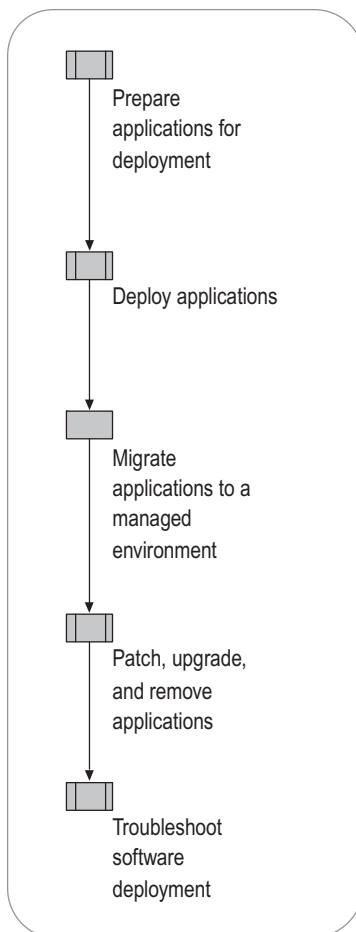
The software installation extension of Microsoft® Windows® Server 2003 Group Policy enables you to create a controlled environment, providing on-demand software installation and automatic repair of applications. Users benefit from reliable access to the applications that they need to perform their jobs on any computer they use on their network.

For worksheets to assist you with the deployment processes discussed in this book, see Additional Resources, later in this chapter.

Deploying a Managed Software Environment Process

The software administrator needs to manage software throughout all phases of the software administration life cycle. Managing this life cycle can shorten the time it takes to deploy software, and can increase the productivity of users. Figure 8.1 illustrates the process for deploying a managed software environment by using Group Policy-based software deployment.

Figure 8.1 Deploying Managed Software



Assessing Microsoft Software Management Solutions

Microsoft offers several software solutions for your networked users. Your organization might already have objectives and requirements for a software installation and management product. Before you plan your deployment, you must verify those objectives to be certain that you use the appropriate technologies for software deployment.

Group Policy, which is built-in to Microsoft® Windows® 2000 and later operating systems, offers a convenient method for distributing software in your Active Directory® directory service environment, especially if you are already using Group Policy for other purposes, such as securing your client and server computers. However, a Group Policy-based software installation has some basic limitations, including difficulties with scheduling installation, consistently managing network bandwidth, and providing feedback on the status of the installation. If you need to carefully schedule installations, manage network use, perform hardware and software inventory, or monitor installation status, consider using Microsoft® Systems Management Server (SMS). For more information about SMS, see the Microsoft Systems Management Server link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources/>.

Using the right solutions can benefit your organization by giving you a centralized, efficient means to perform routine tasks such as updating software. Table 8.1 compares the various software management technologies.

Software installation extension of Group Policy You can use the software installation extension of Group Policy to deploy and manage software if your organization is small or medium in size, and the following conditions exist:

- You have deployed Active Directory.
- You have determined that Group Policy provides the management features your organization requires.
- You have a solid base of client computers running Microsoft® Windows® 2000 Professional or Windows® XP Professional and member servers running Microsoft® Windows® 2000 Server and Windows Server 2003.

**Note**

Your servers do not have to run Windows Server 2003 for you to use Group Policy.

Group Policy can also serve the needs of large enterprises that use other software installation solutions, such as SMS, from the top level across the organization. Consider using Group Policy for distributing software within various groups, such as individual divisions, where you might not need the advanced capabilities of SMS.

Software Update Services You can use Microsoft® Software Update Services (SUS) to quickly acquire and distribute critical Windows patches to computers in your organization. By using SUS, you can choose which of the latest critical or security patches to download, test them in a company-standard operating environment, and then efficiently deploy the patches to the appropriate computers running the Automatic Updates client. For more information about using SUS, see “Deploying Software Update Services” in this book.

Systems Management Server You can use Systems Management Server (SMS) if any of the following conditions exist:

- Your organization is medium or large in size.
- Your users are running operating systems earlier than Windows 2000 Professional.
- You require more advanced capabilities for planning, scheduling, distributing, and tracking software.

The advanced capabilities of SMS include such features as inventory-based targeting, status reporting, server-side and client-side scheduling, multisite facilities, centralized hardware and software inventory, remote diagnostic tools, software metering, software distribution-point population and maintenance, support for Microsoft® Windows® 95, Windows® 98, Windows NT® 4.0, Windows 2000, and Windows® XP clients, and enhanced software deployment features. Additionally, SMS does not require Active Directory. For more information about SMS, see the Microsoft Systems Management Server link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Terminal Services You can use Microsoft® Terminal Services if you have Windows-based desktop applications that require frequent updates, and the users who require those applications are in remote locations and have low bandwidth. When used as a terminal server, a server becomes a Windows application server. This allows the user to run Windows-based applications remotely on the server while only the mouse, keyboard, and display data are transmitted to the local computer. By using Terminal Services, you can offer your users software as a remote service instead of as a local installation package. For more information about using Microsoft® Terminal Services, see “Hosting Applications with Terminal Server” in *Planning Server Deployments* in this kit.

Table 8.1 Comparing Software Management Technologies

Management Function	Group Policy	SMS	Terminal Services	SUS
Patch and upgrade Windows XP, Windows Server 2003, and Windows 2000	N/A	Yes When using SMS for software management, also use it to patch your Windows systems instead of SUS.	Although Terminal Services does not automate patching, you can use it to remotely log on and apply patches.	Windows patches only (no upgrade)
Consistent user environment (persistence of data, software, and settings)	Yes	Software only	Yes	N/A
Disaster recovery for applications in Windows 2000 and Windows XP	Yes	Yes	N/A	N/A
Inventory, advanced deployment, troubleshooting, and diagnostic tools	Limited	Yes	Limited	None
Manage environments that are not Active Directory-based	No	Yes	Yes	Yes (Windows patches only)

Although all these Microsoft management technologies provide important software distribution capabilities, SMS is the preferred Microsoft software distribution solution for medium-sized, and especially for enterprise-sized, organizations. SMS provides advanced features for deploying and managing software, Windows patches, and critical updates. If you use SMS as your software management solution, use the SMS Feature Pack, instead of SUS, to distribute patches and critical updates to your clients. However, SUS, used with the Automatic Updates client, is the recommended solution for distributing Windows patches in conjunction with Group Policy–based software distribution.

Although there are certain instances where you would choose one software deployment method over another, you can also use many of these Microsoft technologies together, depending on your needs. For more information about using these Microsoft software deployment methods to provide a combined solution, see the Application Deployment link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Group Policy Software Deployment Background

To deploy software using Group Policy, you must have an Active Directory–based domain and Windows 2000 or Windows Server 2003 domain controllers. Also, the clients must run Windows 2000 Professional or Windows XP Professional. By using other Windows Server 2003 features and technologies, such as those described in Table 8.2, you can take full advantage of Group Policy-based software deployment.

Table 8.2 Essential Tools and Components for Deploying Software in a Managed Environment

Component or Tool	General Description	Combined with Group Policy Software Installation Extension
Active Directory	A hierarchical collection of objects including domains, sites, OUs, users, computers, and printers that allow an organization to manage these resources.	Provides the scope of management mechanism to locate users and computers. Stores software deployment information through Group Policy.
Group Policy	An administrative tool for defining and controlling the way programs, network resources, and the operating system work for users and computers in an organization. In an Active Directory environment, you apply Group Policy to users or computers on the basis of their membership to sites, domains, or OUs.	Enables you to deploy applications in a Group Policy object (GPO) associated with one or more Active Directory containers, such as sites, domains, or OUs. Use the software installation extension of the Group Policy Object Editor Microsoft Management Console (MMC) snap-in to deploy applications.
Windows Installer	A service based on an operating system, which provides software installation services using a standard package format. You can use Windows Installer to manage the installation, modification, upgrade, and removal of software applications.	Installs, modifies, upgrades, and removes software applications.

(continued)

Table 8.2 Essential Tools and Components for Deploying Software in a Managed Environment (continued)

Component or Tool	General Description	Combined with Group Policy Software Installation Extension
Software installation extension of the Group Policy Object Editor MMC snap-in	An extension of the Group Policy Object Editor MMC snap-in that includes a user interface that allows administrators to deploy and manage software.	<p>Communicates with Active Directory, GPOs, and Windows Installer to assign or publish applications as follows:</p> <ul style="list-style-type: none"> • Assigns software to users. Installs user-assigned applications entirely the first time the user logs on after deployment, or allows users to install certain components or features of an application as needed. • Assigns software to computers. Installs an application the next time the computer starts. The application is available for all the users on that computer. • Publishes applications for users only: Users can choose to install the software from a list of published applications located in Add or Remove Programs in Control Panel.
Group Policy Management Console (GPMC)	A new tool that consists of an MMC snap-in and command-line tools. This tool unifies management of all aspects of Group Policy across an enterprise. GPMC allows you to manage all GPOs, Windows Management Instrumentation (WMI) filters, and permissions on your network.	<p>Group Policy Modeling (formerly known as RSoP planning) allows you to run hypothetical scenarios to verify software configurations under various sites, domains, and OUs. Provides printable HTML reports.</p> <p>Group Policy Results (formerly known as RSoP logging) verifies which software applications are properly installed for a specific group of users or computers. It also pinpoints the causes of unintended removal or damage to software. Provides HTML printable reports.</p>
Add or Remove Programs	A user interface in Control Panel of Windows XP Professional and Windows 2000 Professional. Add or Remove Programs lets users manage software on their own computers.	Lists both published and assigned applications so that users can install, modify, and remove software from their desktop computers.

(continued)

Table 8.2 Essential Tools and Components for Deploying Software in a Managed Environment (continued)

Component or Tool	General Description	Combined with Group Policy Software Installation Extension
Command line and Graphical User Interface (GUI) tools or scripts	These include GPResult.exe, GPOTool.exe, GPOUpdate.exe, ReplMon.exe, NetDiag.exe, InstallShield, and the new Group Policy Management MMC snap-in. Some are installed by default; others must be installed manually.	Helps you manage, optimize, or troubleshoot Group Policy-based software deployment.

The software installation extension of Group Policy allows you to centrally manage the installation of software on all client computers in your organization. You do this either by assigning applications to users or computers, or by publishing applications for users.

Assign software on a per-user or per-computer basis when you do not want to give users the choice to install or remove the software. For example, if a user accidentally removes a user-assigned application by using **Add or Remove Programs**, the software installation extension of Group Policy automatically reapplies the advertisement information after the user logs on or the computer restarts, and the software is reinstalled the next time a user selects it. It is not possible for a user to delete a computer-assigned application. In most cases, packages that you assign to users or computers include applications that are essential but do not create congestion between the clients and the software distribution points.

If you use Group Policy-based software deployment, you can publish software for users only (not available for computers). When you publish software for users, you give them the opportunity to decide if and when they want to install it. They can install the software from a list of published applications in **Add or Remove Programs** in Control Panel. For example, not everyone in the organization requires software for project management. Therefore, a software administrator is likely to publish a project management package for only those users who require it. Managers who require the software can then choose to install it.

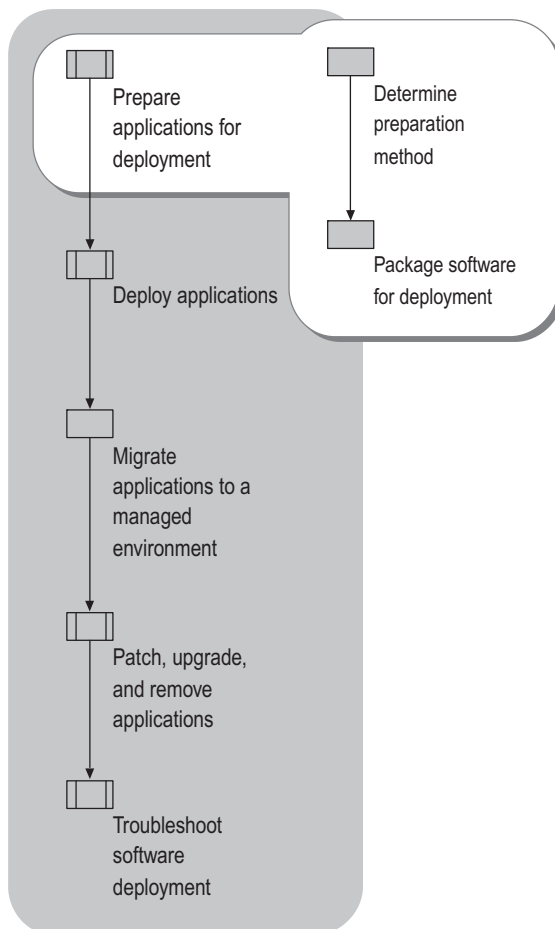
Users can always see both assigned and published applications in **Add or Remove Programs**.

For more information about assigning software to users and computers and publishing software for users, see “Assigning and Publishing Software” later in this chapter.

Preparing Applications for Deployment

Windows Installer is the engine for deploying software packages when you use the software installation extension of Group Policy. It is a core service of the Windows operating system, which enables software administrators to manage the state of software applications. The process of preparing applications involves determining the appropriate packaging method, as indicated in Figure 8.2.

Figure 8.2 Preparing Applications for Deployment



Windows Installer technology uses the following two components to help you install and manage software:

- A Windows Installer package (an .msi file), which is a database containing information that describes the installed state of an application. The Windows Installer package performs the installation, modification, and removal of the software.
- An application programming interface (API) that allows applications and management tools to interact with Windows Installer to install or remove additional features of the application after the initial installation is completed.

The managed state of an application includes installation, modification, upgrade, or removal. Windows Installer provides you with consistent and reliable methods to customize installations, update and upgrade applications, and resolve configuration problems. It can assist you as follows:

- Helps you manage the state of software during and after installation.
- Defines a standard format for application setup and tracks components such as groups of files, registry entries, shortcuts, and other aspects of the application that must be managed together.
- Detects whether software is installed correctly or whether a program file is missing. It can immediately reinstall the damaged or missing files.
- Repairs applications and ensures that they are installed or removed without overwriting or deleting files that are required by another application.
- Enables you to modify an installation by adding or removing features after the installation.
- Enables you to deploy 32-bit and 64-bit Windows applications (Version 2.0).

**Note**

Versions of Windows Installer earlier than version 2.0 can install and manage 32-bit Windows Installer packages only on 32-bit operating systems. Windows Installer version 2.0 supports all of the setup functionality that is available in earlier Windows Installer versions.

Determining the Preparation Method

Before you start the software distribution process, determine which preparation method to use for each new application, patch, or upgrade that you plan to deploy. The following methods are available:

- **Use native Windows Installer packages.** If the application you are installing includes a built-in .msi package you can either deploy the software as-is, or customize it further. For information about using transforms for customizing Windows Installer packages, see “Packaging Software for Deployment” later in this chapter.
- **Reauthor the setup program to include a native .msi.** This method is not recommended except for expert Windows Installer package authors. However, when used, this method is most appropriate if the application is relatively simple, or you have thorough knowledge of its structure and of the application setup on the Windows platform that uses Windows Installer. For more information about reauthoring applications for Windows Installer, see “Packaging Software for Deployment” later in this chapter.
- **Create a Software Installation Settings (.zap) file.** A .zap file is a text file similar to an .ini file, which contains instructions that allow Windows to publish an application (Setup.exe) for users to install by using **Add or Remove Programs** in **Control Panel**. To publish applications that do not install by using Windows Installer, you must create a .zap file, copy the .zap file to the software distribution point servers, and then use the Group Policy–based software deployment to publish the application for the users. You cannot use .zap files for assigned applications.

For information about using other installing programs see article 231747, “How to Publish non-MSI Programs with .zap Files,” in the Microsoft Knowledge Base. To view this article, see the Microsoft Knowledge Base link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Repackaging applications into an .msi format has limitations and application manufacturers typically do not support it. Therefore, consider repackaging as a last resort, except for applications that are developed specifically for your organization. For information about repackaging applications for Windows Installer, see the *Distributed Services Guide* of the *Windows Server 2003 Resource Kit* (or see the *Distributed Services Guide* on the Web at <http://www.microsoft.com/reskit>).

Table 8.3 describes the advantages and disadvantages of the various packaging methods.

**Note**

Packages that are created on Windows 2000 by using Veritas WinInstall LE (the repackaging software that is included with Windows 2000) work on target computers running Windows XP. However, Veritas WinInstall LE does not run on Windows XP and is not intended for repackaging new .msi files.

Table 8.3 Comparing Packaging Methods

Advantages and Disadvantages	Natively Author or Reauthor Windows Installer-Based Packages	Repackaging	.zap Files
Advantages	<p>Can benefit from all Windows Installer features, including just-in-time feature installation, feature repair, and installation with elevated permissions.</p> <p>Can be run without user intervention.</p> <p>Can be assigned or published.</p> <p>Does not require user to be a local administrator to install.</p> <p>Can automatically repair itself if key files are damaged or missing.</p> <p>If application includes native .msi package, easy to deploy.</p> <p>Can roll back an unsuccessful installation, modification, repair, or removal.</p>	<p>Same benefits as natively authoring.</p>	<p>Easy to create and fast to deploy.</p> <p>Display application in Add or Remove Programs.</p>
Disadvantages	<p>Time-consuming to build and test.</p>	<p>Can easily fail if repackaging not performed on a clean computer.</p> <p>Time-consuming to build and test.</p> <p>Control over installation less detailed than natively authoring.</p>	<p>Run existing setup, requiring user intervention.</p> <p>Do not benefit from Windows Installer features.</p> <p>Might require user to have local administrator permissions to install.</p> <p>Cannot automatically install software or features on demand.</p> <p>Cannot automatically repair if key files are damaged or missing.</p> <p>Cannot roll back an unsuccessful operation.</p>



Important

Before you reauthor or repack applications in your organization:

1. Check with the application manufacturer or internal development group to see if either has or is planning to develop a native Windows Installer implementation of the program.
2. Weigh the benefits of reauthoring and repackaging against the costs involved. Keep in mind that both are advanced operations. There are tools for each operation that can help software package developers create the final Windows Installer package, but the procedures are still quite resource-intensive and can be costly.

Packaging Software for Deployment

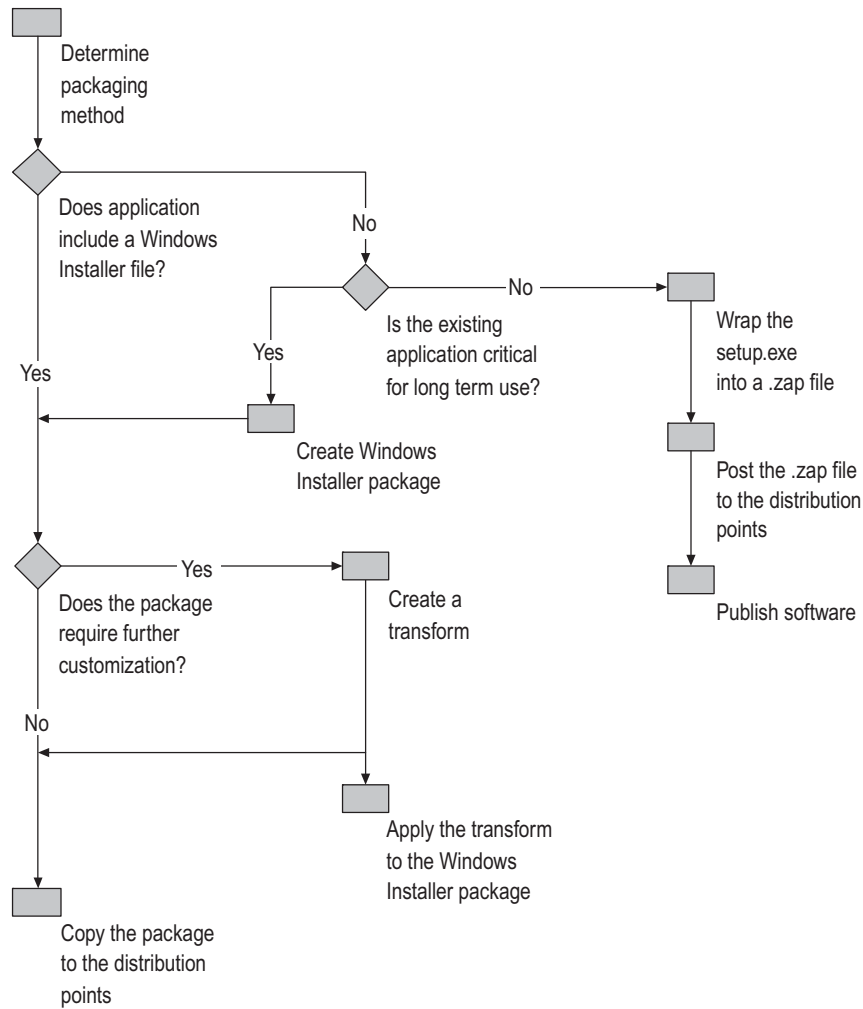
Each time you use the software installation extension of Group Policy to deploy an application, patch, or upgrade package, you must first prepare the application for Windows Installer. If the application does not include a natively authored Windows Installer package (.msi), you must obtain one or create a .zap file.

Each Windows Installer package file contains a database that stores all the instructions and data that are required to manage the state of a program. For example, an .msi file of an application might contain instructions for installing the application when an earlier version of the application has been installed. The .msi file might also contain instructions for installing the software on a computer where that application has never been installed.

To package software, you might only have to perform an administrative installation to prepare the application for later installation by client users or computers from a network location. However, you might want to customize the application deployment so that you can create a transform that modifies the .msi. Also, if your application does not include a Windows Installer package, packaging can be much more complex. In that case, you must determine how long your organization expects to use the application. Your decision might lead you to reauthor the Setup.exe file of the application.

Figure 8.3 illustrates the process for packaging software for deployment by using Windows Installer and the software installation extension of Group Policy.

Figure 8.3 Packaging Applications for Deployment



Using Native Windows Installer Packages

Many software authors develop applications to include native Windows Installer packages. A native Windows Installer package contains a single product, such as Microsoft® Office 2000, which can be made up of several features, such as Microsoft® Word, Microsoft® Excel, and Microsoft® PowerPoint®. However, you can configure the software to install features individually. When the user selects an uninstalled feature, the feature is installed. Each feature (Word, Excel, PowerPoint, and so on) contains components, such as a thesaurus, spelling checker, or an additional user-interface language. When the user selects a feature or component that is not installed, the feature or component is automatically installed. Automatic installation of selected features saves network bandwidth during the initial installation. It also gives users only the features and components that they need to do their jobs. Automatic installation can also save space on users' local disk drives. However, this type of installation delays the availability of a feature when the user first selects it.

Windows Installer packages ensure that an accidentally deleted file, such as Winword.exe, is reinstalled the next time the user tries to start Word because Windows Installer detects and reinstalls missing files.

After you obtain a native Windows Installer package, perform one of the following tasks if the application you plan to deploy includes a native Windows Installer package:

- If the package requires no further customization, copy it to the designated shared folders on the software distribution point servers.
- If you want to modify the .msi package use transforms to customize it.

For information about copying packages to the software distribution servers, see “Deploying Applications in a Managed Environment” later in this chapter.

Customizing Windows Installer Packages by Using Transforms

A *transform* (.mst file) is a collection of specified changes that you apply to a base Windows Installer package file at the time of deployment. After you package the software in the Windows Installer package format, you can use transforms to customize the software for your organization. At this phase, the modular design of Windows Installer packages simplifies deployment. When you apply transforms to an .msi file, Windows Installer can dynamically add or modify data in the installation database to customize the installation of the application.

Office 2000, for example, provides the Office 2000 Custom Installation wizard, which you can use to build transforms. You can create a transform for managing the configuration of Office 2000 that you deploy to users in your organization. Other tools in the Windows Installer SDK, or other non-Microsoft tools, can also help you to create transforms for Windows Installer packages that do not include their own custom installation tools.

Purposes for Transforms

Transforms tailor the installation of an application. Although they are optional, you can use transforms for a variety of purposes including encapsulating and customizing.

Customizing

Customizing can involve configuring installations so that a particular set of features from a specified software application, or suite of software applications, is installed locally on the computer.

You can also use transforms to add new features to an existing application's package. For example, you can add custom Excel templates for the Finance group. However, if the templates change frequently, it might be a better practice to package them, and then assign or publish them as a separate package.

Encapsulating

You can encapsulate numerous customizations of a base package that are required by different groups. For example, in organizations where the Finance and Marketing departments require different installations of a product, you can make the product's base package available to everyone at one software distribution point. Then you can distribute the appropriate customizations separately as transforms to each group of users.



Important

Store transforms at the same software distribution point and in the same shared folders as the Windows Installer package that they customize or the installation will fail.

Customizing a Native Windows Installer Package Example

An organization maintains a large number of applications. Some of these applications contain native Windows Installer packages that require some customization, and many of the applications require modification to prepare them for Windows Installer. The Finance and Marketing departments of the organization require different installations of a custom-designed customer database application that includes a native Windows Installer package (.msi). The Finance department requires financial information about customer accounts, and the Marketing department requires customer purchase history to determine the best use for marketing resources.

The software administrator made the application's base package available to everyone from one software distribution point, and then distributed the appropriate customizations to each group of users separately as transforms. To achieve this, she did the following tasks:

1. Copied the original .msi to the designated software distribution point servers.
2. Created two separate transform files (.mst), each containing the customizations for the Finance and Marketing departments.
3. Copied the .mst files to the same shared folders on the software distribution point server where the original .msi files are located.
4. Created a `GPO ` and assigned the application to the users in both the Finance and Marketing departments.

When users log off and log on again, the application is published on their desktops, and it is also listed under **Programs** on the **Start** menu.

You associate a transform with a Windows Installer package by using a GPO when you first deploy the package.

► **To associate a transform with a Windows Installer package by using a GPO**

1. Select the software installation extension of the Group Policy object.
2. In the right pane of the Group Policy Object Editor, right-click the managed software.
3. Click **Properties**.
4. In the appropriate fields on the **Modifications** tab, specify the modifications or transforms that are associated with the package.



Important

Do not change the manufacturer's product code for the package when you create a transform to customize a native Windows Installer package. The software installation extension of Group Policy treats the new code as a new product. This can cause a failed installation and void your licensing agreement.

Modifying a Transform

To modify a transform by using the software installation extension of Group Policy, you can create an upgraded relationship between the application and the old transform, or between the application and the new transform. An appropriate time to do is this when you create a new transform or when you distribute new software that requires a transform.

► **To modify a transform**

1. Create a new .mst file.
2. Remove the existing associated .mst files by using the software installation extension of the Group Policy Object Editor.
3. Associate the new .mst file by using the original .msi.



Important

Remember that a transform is applied at the time of assignment or publication, not at the time of installation. Verify that the **Modifications** tab of the package properties dialog box is properly configured *before* you click **OK**. If you do not do this, and you deploy an incorrectly transformed package, you must either remove the software and redeploy it, or upgrade the software to a correctly transformed version.

After Modifying a Transform

After you create or modify a transform, you must deploy the new transform.

► **To deploy a new or modified transform**

1. Copy a new .msi file and a new .mst file to the designated shared folders on the software distribution point servers.
2. Delete the existing package object from the software installation extension of the Group Policy Object Editor.
3. Associate the new .mst file with the original .msi file.
4. Deploy the new package and the transform at the same time.

For information about copying software to the software distribution point servers, see “Deploying Applications in a Managed Environment” later in this chapter.

Reauthoring Applications for Windows Installer

When you reauthor an application, you create an application that adheres to the Windows Installer format. You are essentially redeveloping the setup portion of the application to take full advantage of the advanced capabilities of Windows Installer.

If you plan to reauthor an application that does not include a Windows Installer package, you must have the following:

- All executable files, dynamic-link library (DLL) files, and other resources. For all but the simplest applications, you need the source code to understand the logic and actions of the original setup program.
- An understanding of the application and the registry entries, shortcuts, and other information that are needed for it to run correctly.
- An authoring tool that supports creating Windows Installer packages.

There are some authoring tools available to help developers create new Windows Installer packages, but the procedures can be resource-intensive and costly. If you determine that the application will play a key role in the future of the company, it is important to weigh the benefits of reauthoring the application with the costs of reauthoring the application.

Tools to Help You Create Windows Installer Packages

Several tool vendors supply .msi package-authoring tools that developers can use to create Windows Installer packages. Such authoring tools include, but are not limited to:

- Microsoft® Visual Studio® Installer
- Microsoft® Visual Studio® .NET
- Commercial installers for Windows



Tip

To develop any new or custom applications for your organization, use Windows Installer technology during the design phase. By designing the application with Windows Installer in mind from the outset, you can take full advantage of Windows Installer capabilities.

If you plan to reauthor an application to include a Windows Installer package, see the Windows Installer Software Developer's Kit (SDK) link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>

For more information about the Microsoft® Visual Studio® Installer authoring tools for installing software, see the Microsoft Visual Studio Installer link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>

After Reauthoring Applications for Windows Installer

After you have reauthored an application to include a Windows Installer package, the next step is to perform one of the following tasks:

- If the package requires no further customization, copy it to the designated shared folders on the software distribution point servers.
- If you want to customize the .msi package for your users, use transforms (.mst files) to modify it.

For information about copying packages to the software distribution point servers, see “Deploying Applications in a Managed Environment” later in this chapter.

Reauthoring an Application for Windows Installer Example

Administrators have developed a simplified custom application so that users can arrange their own business travel. Because the application was developed internally, the organization has all the files for the software, and the developers understand how the software must be installed. IT management determined that this application is ideal for reauthoring packages for Windows Installer.

To reauthor the business travel application, the administrator performed the following tasks:

1. Compared the benefits of having the application with the costs to reauthor it.
2. Identified the developers to perform the task of reauthoring the application.
3. Chose the appropriate reauthoring tool.
4. Reauthored the application to include a native Windows Installer package.
5. Placed the native .msi on the software distribution point.
6. Created a GPO and published the application for a particular group of users.

Users who need the business travel application can go to **Add or Remove Programs** in Control Panel, and then download the software from a published list of applications.

Creating .zap Files

Applications that do not use the .msi file format for the Windows Installer Service can be set up for distribution by creating a text file that has a .zap file extension. This method is not as flexible as .msi package files. If you have many applications that do not contain native Windows Installer packages, and you know that your organization plans to discontinue these applications, you can create software installation settings (.zap) files for the installation executable (such as Setup.exe or install.exe) files. Additionally, if you use custom applications that do not have Windows Installer support, but you plan to use them in the long term, .zap files might be your only choice. When you create .zap files, you do not benefit from the capabilities of Windows Installer. By creating .zap files, you wrap 32-bit or 64-bit Setup.exe files into a .zap file format that the software installation extension of Group Policy recognizes. This method allows you to publish the applications for users to install by using **Add or Remove Programs**.

Because these applications do not use Windows Installer setup programs, they do not do the following:

- Use elevated permissions for installation.
- Install a feature on the first use of the feature.
- Roll back an unsuccessful operation, such as install, modify, repair, or removal.
- Detect a broken state and automatically repair it.
- Implement customized installations (transforms).

Suggestions for Working with .zap Files

When you work with .zap files, consider the following:

- While applications that are installed by using .zap files run their original setup programs, they do not run with the elevated permissions that Windows Installer packages have. If installing the application requires administrative permissions, only users who have those permissions can install it.
- Because .zap files are typically created by using text editors, the files might have a .zap.txt file name extension. Make sure that the file name extension of a .zap file is only .zap (without the .txt extension). Also, make sure that any software installation file that you distribute by using GPOs does not end in .txt.
- If you have 64-bit clients, test 32-bit .zap applications to verify that you can install and run them on 64-bit clients. This is important because more .zap applications fail on 64-bit clients than on 32-bit clients.
- Unless you change the default behavior, 32-bit .zap applications are deployed so that they are not listed in **Add or Remove Programs** on 64-bit clients.

After Creating .zap Files

After you create a .zap file, copy it to the designated shared folders of the software distribution point servers. You can then use the software installation extension of Group Policy to publish the application in **Add or Remove Programs** in Control Panel. This makes the application readily available to users. You cannot customize .zap files by using transforms.

Creating a .zap File Example

The software administrators of the organization have identified a group of users who use an Excel template that is only compatible with Microsoft® Excel 97. Although all other users in the organization plan to upgrade to Microsoft® Office XP, this group of users must continue using Excel 97 until the end of this particular project. Excel 97 does not include a native .msi package file. After this project is completed, this organization has no further need for Excel 97.

To make sure that these users have Excel 97, the administrator performed the following tasks:

1. Wrapped the setup program of Excel 97 into a .zap file.
2. Copied it to the designated software distribution point servers.
3. Created a GPO and published the software to that particular group of users.

The users who need Excel 97 can now go to **Add or Remove Programs** in Control Panel, and then download the software from a published list of applications.

To publish Excel 97 by using the existing Excel 97 setup program, only the three path-information lines are needed in a .zap file. The following example represents the .zap file that the software administrator created for the purpose of deploying Excel 97 to the users on this project.

```
Path information <Application>
FriendlyName = "Microsoft Excel 97"
SetupCommand="\"server\share\Excel 97\setup.exe"
```

The path and the name of the .exe file are enclosed in quotation marks in the Application section. If there are no command-line arguments, the .exe file path and name must be enclosed in two sets of quotation marks. For example:

```
Absolute path SetupCommand="\"server\share\long folder\setup.exe" /argument
SetupCommand="\"server\share\long folder\setup.exe"

Relative path SetupCommand="setup.exe" /argument
SetupCommand="\"setup.exe"
```



Note

When you create your own .zap file, modify the information in the preceding sample .zap file according to the application that you are managing and the location of your software distribution point.

For more information about publishing .zap file-packaged applications, see “Targeting Software to Users and Computers” later in this chapter.

Packaging 64-Bit Applications

In the Windows Server 2003 family of servers, the software installation extension of Group Policy and Windows Installer 2.0 continue to support and protect the investment that you have made in 32-bit applications. Additionally, Microsoft® Windows® Server 2003, Enterprise Edition and Windows® Server 2003, Datacenter Edition introduce support for 64-bit application installation.

Windows Installer version 2.0 installs three types of Windows Installer packages on a computer running a 64-bit operating system:

- 32-bit packages that contain only 32-bit components
- 64-bit packages containing some 64-bit components and some 32-bit components
- 64-bit packages containing only 64-bit components



Note

You cannot publish or install a 64-bit application on a 32-bit operating system.

You can use the Software Installation extension of Group Policy to allow or disallow installation of 32-bit applications to 64-bit clients.

► To allow or disallow installation of 32-bit applications on 64-bit clients

1. Open the Group Policy Object Editor to the Software Installation item.
2. Right-click the managed software, and then select **Properties**.
3. On the **Deployment** tab, click **Advanced**.

You might decide not to deploy a 32-bit package to a 64-bit system if that application functions poorly or not at all on 64-bit systems. Make your configuration determinations as you test the applications and system combinations in your test lab and during your pilot phase. For more information about piloting the deployment of applications, see “Conducting a Pilot for Software Deployment” later in this chapter. For guidelines about testing the applications in your organization, see “Planning and Testing for Application Deployment” in *Planning, Testing, and Piloting Deployment Projects* in this kit.



Important

Do not deploy a 32-bit application that uses the same Windows Installer 2.0 Product ID as a 64-bit application. Instead of creating such Windows Installer 2.0 packages, create a separate Product ID for the 64-bit version of a product. Windows Installer does not support different architecture packages that have the same product code.

If you incorrectly configure a 64-bit package for 32-bit clients (or use the wrong Product ID), Group Policy tries to install it, but then removes the package at logon. It then installs the package again the next time a user logs on, and then removes it again, creating network traffic and preventing users from using their computers.

Repackaging Applications for Windows Installer

When you cannot reauthor a package to use Windows Installer, you might want to repackaging it. Repackaging an application for Windows Installer involves taking a snapshot of a clean computer (including the registry settings, files, and system settings), installing the software, and then taking a post-installation snapshot of the computer. The repackaging software detects the difference between the two snapshots, and then creates the necessary instructions to reproduce the installation. If any registry changes, files changes, or system setting changes occur during the capture process, they are included in the installation. You use repackaging when you do not have control over DLL files, source code, and registry entries, or for applications about which you do not have in-depth knowledge.

Use this method only as a last resort when you need to repackage an application into an .msi. It is easy to underestimate the cost of repackaging in terms of labor hours. Also, users often set their expectations too high for the reliability of repackaged applications. Repackaging requires a thorough knowledge of the application's installation program and of the Windows Installer setup on the Windows platform.

Success with repackaging is affected by the state of the computer where you perform the repackaging. For best results, always perform a repackaging by using a clean computer. For the purpose of repackaging, a clean computer is defined as a computer that has only the operating system and operating system service packs installed before you run the repackaging software. Because of this limitation, and other issues, repackaging is not recommended.

Repackaging is not a function or a feature of Windows Installer. As with reauthoring applications, several vendors provide tools to enable administrators to repackage applications for a variety of needs. The same vendors who provide tools to reauthor applications can also help you repackage them.

When you repackage an application, you replace the existing components, such as DLLs, .ini files, registry settings, and shortcuts, and then you create a path for Windows Installer to find these items at installation time.

Packages that you create on a computer running Windows 2000 by using Veritas WinInstall LE, will work on target computers running Windows XP. However, the Veritas WinInstall LE program itself does not run on Windows XP. For more information about repackaging applications on newer computers, contact your repackaging-software vendor.



Important

- Microsoft supports authoring and customizing applications that natively use Windows Installer for installation and maintenance. However, Microsoft does not provide support for applications that are repackaged as .msi files. Contact the application manufacturer for this type of support.
- As with other repackaging techniques, repackaging applications into the Windows Installer format has limitations and might not be supported by the application manufacturer. For more information, contact each application manufacturer.

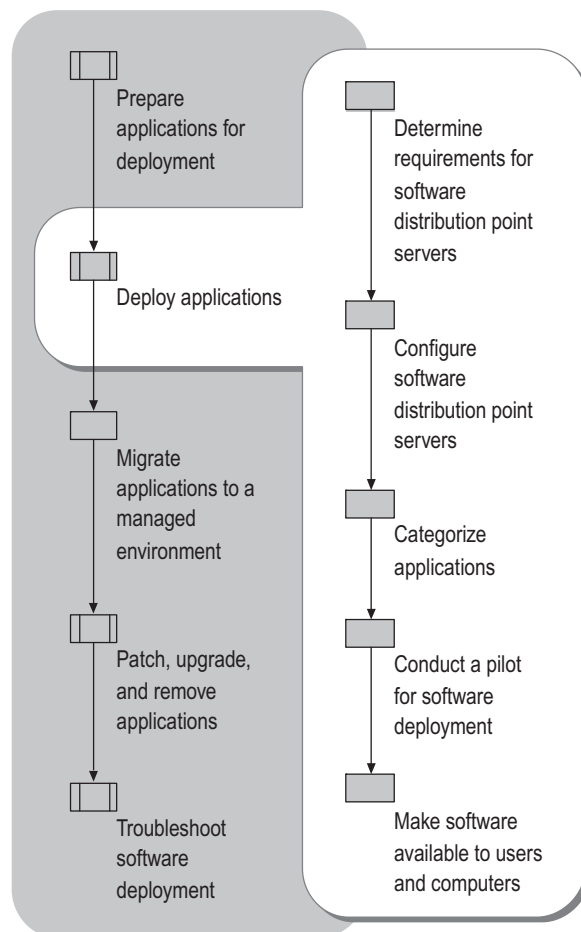
If you have an application that does not include a native Windows Installer package, and you decide to repackage it in the .msi format, see the Windows Installer SDK for detailed documentation about the Windows Installer package format. For more information about the authoring tools for deploying a managed software environment, see the product links, as listed by product name, on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

After you repackage an application for Windows Installer, copy it to the designated shared folders of the software distribution point servers. You cannot customize repackaged applications by using transforms.

Deploying Applications in a Managed Environment

After you prepare the application for deployment, you can deploy the software by using Group Policy or another software distribution technology. Each time you deploy applications, patches, or updates in your test environment, and then to the rest of the organization, you must prepare the software for Windows Installer. You are then ready to perform the tasks as listed in Figure 8.4.

Figure 8.4 Deploying Applications



Deploying applications is the process of setting up and managing distribution points or server shares where users have access to the packaged software and can install it on their computers. Before you can begin distributing applications, you must clearly understand the current arrangement of servers and client computers on your network, the software requirements of users, and their locations on the network. Also, plan for who will install and manage the software.

Microsoft Distributed File System (DFS) and File Replication service (FRS) can enhance the security and availability of your distribution points. For more information about DFS, FRS, and Microsoft file-server technologies, and how to best deploy these technologies, see “Designing and Deploying File Servers” in *Planning Server Deployments* of this kit. This is an important topic to understand before you deploy your Group Policy–based software distribution solution. Read that chapter before you configure your distribution point servers.

Whether you decide to use DFS, FRS, or another method to configure your distribution point servers, you can distribute software to users by using the software installation extension of Group Policy.

Network traffic can become excessive when clients simultaneously download software. To prepare for this load, perform the following tasks before you place software distribution point servers on your network:

- Identify the users’ software requirements and where these users are located.
- Examine the network infrastructure:
 - Measure network capacity and bandwidth.
 - Identify the slow or intermittently connected network links.
 - Identify performance issues between clients and software distribution point servers.
- Plan for securing your software distribution point servers.
- Evaluate using DFS and FRS as supporting technologies for Group Policy-based software distribution.

Identifying Software Requirements and Locations of Users

When you know what software users require and where those users are located on the network, place the software distribution point servers close to those users (on the same subnet, for example). If you have users who connect over slow links, consider the impact to the network performance if you allow them to download software over those slow links.



Note

If you are deploying the same application to clients at two locations, deploy it by using two targeted GPOs instead of one. One of the GPOs applies to all clients at one location and uses a UNC path to a source point at that location. The other GPO applies to all clients at the other location and uses a UNC path to a source point at that location. GPOs can be linked to Active Directory sites, which can be a valuable option in this context.

Examining the Network Infrastructure

When you are familiar with the network infrastructure in your organization, you can determine which method for managing software distribution point servers is best for your organization. If you use DFS and FRS, you must understand your network infrastructure to design your DFS namespace, replication topology, and replication schedule. For more information about using DFS and FRS, see “Designing and Deploying File Servers” in *Planning Server Deployments*.

Measuring network capacity and bandwidth

You can measure network capacity by determining the number of connections that the server establishes and maintains. Available bandwidth varies widely, depending on the transmission capacity of the link, the server configuration, the server workload, and competing traffic. The capacity of a single server changes during operation in response to demand and competition for shared network resources.

With the fluctuation of server capacity in mind, you must place software distribution point servers as close as possible to the users who need to access them (preferably on local networks). If you implement DFS, you have three options for configuring DFS to select targets: default, restricted, or least expensive.

Default target selection If the last (or only), target in an Active Directory site fails or is taken offline, DFS directs clients to another target in the same site, if a target is available. Clients are directed to a random target if no same-site targets are available. DFS does not consider bandwidth cost or speed when choosing the random target.

Restricted same-site target selection You can limit client access to only those targets that are in the same site as the client. When you use this option, plan to have at least one target (or two targets, for fault tolerance) in every site. If no same-site targets exist, clients in that site are denied access to the data in the namespace.

Least-expensive target selection You can make DFS use an alternate target that is based on connection cost if no same-site targets are available. Windows Server 2003 uses the site and cost information in Active Directory to determine whether sites are linked by inexpensive high-speed links, or by expensive WAN links.

To avoid installation failure, test the replication of application components (the executable files, the Windows Installer packages, and any transforms) from the location of the administrator who is initiating the deployment to all the software distribution points near intended recipients. If an administrator plans to work remotely, be sure to test this configuration. For more information about deploying file servers, see “Designing and Deploying File Servers” in *Planning Server Deployments*.



Important

To ensure reliable transfer and usable connection speed, place frequently accessed data in the same sites as the primary users of the information. You can increase availability by placing multiple servers in each site, as needed.

Identifying slow-link connections

Many remote and mobile users connect to the network by using slow-link connections. The software installation extension of Group Policy can move large amounts of data, so processing across a slow link can affect performance significantly. By default, Group Policy–based software deployment does not operate over slow network or dial-up connections. However, you can allow users to install published applications over a slow link if absolutely necessary. However, you cannot configure Group Policy for automatic assignment, upgrade, or removal of applications over slow links.



Note

A remote access connection is not necessarily a slow link, nor is a local area network (LAN) necessarily a fast link. By default, the fast or slow status of a link is based on a test ping to the server. If it takes less than 2000 milliseconds (two seconds), then it is considered a fast link. If it takes longer than 2000 milliseconds it is considered a slow link. You can set this value by using the Group Policy setting, **Group Policy slow link detection**.

Evaluating Strategies for Connecting Remote Users

If any users connect primarily over slow links, it is essential that you define an appropriate software deployment strategy for them. While keeping the application management objective in the forefront, you can address this challenge by various means:

Terminal Services Run the applications on a server running Terminal Services. This is currently the best method for providing remote computers with access to Windows-based applications that are deployed by using Group Policy-based software installation. The terminal server becomes a single access point that allows multiple users to have access to a desktop where they can download applications, run programs, save files, and use network resources without an administrator having to manage multiple, remote desktops.

When using Terminal Services, administrators install applications on a per-computer basis, meaning that applications are available to any user who has access to the terminal server. Users can gain access to a terminal server over any Transmission Control Protocol/Internet Protocol (TCP/IP) connection including Remote Access, Ethernet, the Internet, wireless, wide area network (WAN), or virtual private network (VPN). The user experience is limited only by the characteristics of the weakest link in the connection. The TCP/IP deployment in the data center governs the security of the link.

For more information about using Terminal Services to deploy applications, see “Hosting Applications with Terminal Server” in *Planning Server Deployments* of this kit.

Direct Installation Have remote and mobile user bring their portable computers to the office so that you can install the software. If you use this method, use the **Install this application at logon** option to install software in its entirety automatically the next time the user logs on to the network. For more information about this option see “Assigning and Publishing Software” later in this chapter. This option will not interfere if mobile users manually install the needed software whenever they have access to a fast link.

Add or Remove Programs Educate remote users to install applications periodically from **Add or Remove Programs** in Control Panel. Any assigned application behaves like a published application when users gain access to it over a slow link. Having remote users installing applications might not be the best method because of the time and bandwidth required, but it lets users decide when to begin the lengthy installations. Keep in mind that, if many users share a slow link, they might block the connection. However, if only a few users share a slow link, this method might provide a practical solution.

SMS Use SMS to deploy software to users who can connect only over slow network links. For example, SMS supports a CD-ROM distribution method by which you can install a distribution package on a CD-ROM, and then send it to mobile or remote users. For more information about providing connectivity for remote and mobile users by using SMS, see the Microsoft Systems Management Server link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Do not use WebDAV to publish software on a Web server. This method can allow an unauthorized user to run a script under the security context of the WebDAV thread, and gain access to your network. See Microsoft Security Bulletin MS01-022 for details.

Identifying performance issues

To understand the performance issues between the client computers and the software distribution point servers in your organization, perform these tasks (not necessarily in this order) in your test lab:

- Determine if the installation of the software is assigned (required) or published (optional), and if the assignment is to users or computers. For example, assigning an application to a large number of users or computers has a heavy impact on the network when a high number of users log on the same day and automatic, simultaneous software downloads start.
- If you publish the application, users can download software as-needed. In effect, publishing staggers the downloading of the software, which decreases congestion on the network.
- Determine how many settings you can include in a GPO and still maintain the balance between settings and logon times. Having many GPOs often increases logon times; logon times are especially affected by the number of settings in those GPOs. Having fewer GPOs is easier to manage but limits flexibility. Testing these configurations in the lab can help you to determine the optimum balance for your organization. It is recommended that you use GPMC to test, stage, and deploy your GPOs.
- Consider the size of each software application that you plan to distribute. Obviously, the larger the application, the larger the impact on the network, especially if you assign the application to a large group of users or computers at one time.
- Consider the placement of the software distribution point server in relation to the targeted users: How long does it take for a particular package to go from a software distribution point server to a client? Test the most common client and server access circumstances, the least common client and server access circumstances, and worst-case situations.

- Plan for the number and frequency of the software deployments. These factors affect the amount of server disk space that is required and the subsequent network load. For example, when many users install a small package simultaneously, a large amount of data suddenly moves across the network. This can have a greater impact on your network than a large package that is rarely installed.
- Consider how many users access a package at one time. In this instance, determine if you will use the **Install this application at logon** option (located in the software installation extension of Group Policy), or if you will use the default option and allow the users to install the application components on an as-needed basis. The following are two instances where large numbers of users might access a package at the same time:
 - **New software package placed on the software distribution point.** In this case, expect a large number of initial installations whether you publish or assign the software. Stagger the installation so that all users do not download packages at the same time on the same day. For example, you can break up the users into small groups and assign a certain application to 500 users one week, and then assign the same application to 500 different users the following week. This minimizes the effect that software installation has on your network bandwidth.
 - **Many new employees starting on the same day.** If this occurs, consider the network overhead for these users to log on and receive assigned packages. Also, consider the number of published packages that these new employees must gain access to over a specified time. After you determine the results in your situation, make decisions that protect your servers from becoming overloaded by providing sufficient software distribution points that are part of a DFS namespace. Note that SMS uses scheduling to avoid this problem.

Test potential issues in a lab to determine what might happen on the network if a specified number of users try to gain access to a specified software distribution point simultaneously to install a 10 megabyte (MB) application, a 50 MB application, a 100 MB application, or a larger application.

After you have determined your network capacity, you have identified slow link connections, and you have identified and resolved performance issues between client computers and software distribution point servers, you must configure the software distribution point servers.

Determining Requirements for Software Distribution Point Servers

The method that works better for deploying and managing software distribution point servers depends on the objectives of your organization. You can use either of the following methods:

- Set up a universal naming convention (UNC) path to a server share.
- Use DFS.

Setting up a UNC Path to a Server Share

By using the UNC names, a user or application can specify the physical server and share names to gain access to file information. For example: `\\Server\Share\Path\File_name`. You can use a UNC path to allow direct access to a shared file by mapping to a network drive, where the drive letter denotes `\\Server\Share`. You can also perform a deep **net use** to navigate beyond the redirected drive.

However, as networks grow and as organizations begin using existing storage for new purposes, mapping a single drive letter to individual shares becomes inefficient. Also, despite the fact that users and applications can refer to UNC names directly, the increasing number of places users must go to retrieve data can be overwhelming.

Using DFS to Manage Your Software Distribution Point Servers

DFS provides fault tolerance for your software distribution points by mapping a given logical name to shared folders on multiple file servers. This way, software remains available for installation, regardless of whether one of the physical servers where the software deployment files reside becomes unavailable. DFS also improves storage scalability because you can deploy additional or higher-performance file servers and present the storage on the new computers as new directories in an existing namespace.

When you use DFS in combination with Group Policy–based software deployment, you benefit from its location independence and load-sharing abilities. These features simplify management and optimize the installation for users. Instead of allowing all users to install software from a single server, and taxing the server, you can design a DFS namespace to distribute network traffic across multiple servers.

For more information about DFS, EFS, and creating a replication topology and schedule, see “Designing and Deploying File Servers” in *Planning Server Deployments*.

Configuring Software Distribution Point Servers

After you place the software distribution point servers, you must configure each server for the software applications that are accessible to users. Configurations include granting the appropriate permissions so that users (for user-assigned applications) and computers (for computer-assigned applications) can gain access to the software.

After you complete the deployment, you cannot change the path to another software distribution point without redeploying the software package. Redeploying software can be quite intrusive to users because it automatically removes the application on computers where the software is already installed. If the software is assigned, it is reinstalled automatically; if it is published, it must be manually selected again for installation by using **Add or Remove Programs** or by opening an appropriate file type.



Important

When you create a DFS software distribution point for a new application, you must specify a different DFS path, regardless of whether the target software is on the same share. You can then retire software distribution points for the old software by taking down targets of the DFS tree while all the new software distribution points of the new application remain available.

To set up a software distribution point server, copy the software and your Windows Installer packages to the designated servers. Perform an administrative install of the software before you distribute it to clients and servers. To perform an administrative install, run the application's Setup.exe from a command line against the application's CD-ROM. Set the **/a** option to the relevant share in the form of *Server Name\Share Name*. This unpacks all the files from the .cab files, and then drops all the packaged files on the target share. You do not have to log on to the software distribution point server. However, any user who performs an administrative install must have administrative access to the destination share.

Typically, you copy the Windows Installer packages to an intermediate location and then run **Setup /a** from there to the destination that you want. Alternatively, you can run **Setup /a** from and to the software distribution share itself. The drawback of this method is that it unpacks the .cab files, and then leaves them on the same share as the Windows Installer package. This method uses space on the share. However, many administrators do this intentionally so that the .cab files are always available from the destination share. This is a matter of preference, or ease of use, and does not affect performance.

When you set up a software distribution point server, be sure to maintain the security of your network by performing the following tasks:

1. Restrict physical access to the server to the administrators who must physically touch the server.
2. Consider using digital signing. For more information about digital certificates, see “Designing a Public Key Infrastructure” in *Designing and Deploying Directory and Security Services* of this kit.
3. Create the folders for the software on the server that you designate as the software distribution point, and then make the folders network shares. For example:
`\\Server_Name\Share_Name`
4. Copy the Windows Installer packages, application executable files, .mst files, .msp files and .zap files (if used) to the appropriate shared folders.
5. Set appropriate permissions on the folders.

If you allow high-level permissions to a very broad group, you increase the chance that your servers might be tampered with. Software distribution point servers can become security hazards in your organization if they are loaded with harmful or damaged software packages. Allow users to read from the software distribution point. However, only grant Full Control to designated software deployment administrators.

Set the following discretionary access control list (DACL) permissions:

- **Everyone:** Read
- **Administrator:** Full Control, Change, and Read. Grant these permissions only to software deployment administrators who must add or modify installation packages on the server. Also, limit access permissions to only those permissions that the administrators need to do their jobs. Note that administrators who have edit rights on a GPO effectively acquire local administrator rights on all computers that receive that GPO to install and remove software, although they do not become local administrators.



Note

You must have software licenses for software that is written by independent software vendors and distributed by software distribution points. It is your responsibility to limit the number of users who gain access to software through software distribution points to the number of licenses that you own. It is also your responsibility to verify that you are working within the licensing requirements that are provided by each independent software manufacturer.

Whether you install applications by using SMS or Group Policy, it is important to understand the implications of software license agreements. Some applications are licensed per seat, and others are licensed per user or per site. The license agreement for an application might influence your choice of installation method and your decision about whether to have Group Policy assign the application to the computer, or whether to assign or publish the application to the user.

Targeting Software

After you distribute prepared applications to the appropriate software distribution point servers, target each application to a list of intended recipients. Recipients can be specified users, groups of users (such as all members of a certain defined OU), computers, or any combination of these.

Typically, administrators define the hierarchical structure of the sites, domains, and OUs for Active Directory. They do this based on an assessment of their organization's business objectives, administrative requirements, and user needs. When you perform your assessment to target software to users and computers, you narrow your scope to the software-based needs of all users in the organization and the administrative requirements for managing the software. It is essential that you consider the Active Directory structure when determining your software deployment strategy.

It is also important that you evaluate each application that you plan to deploy, from the perspective of both the users who need the application and the administrators who will manage it.

► To assess the administrative requirements and business needs of the users in your organization

1. Identify what software is mandatory for your entire organization and what software is appropriate for a particular job or business unit.
2. Identify the users who must have specific language versions of the software.
3. Determine whether to assign the software to users or to computers, or to publish for users. If you assign software to users, decide whether you want the software to install fully after computer startup, or if the on-demand approach works better for your users and your network infrastructure requirements. See "Assigning and Publishing Software" later in this chapter.
4. Identify remote software installation requirements.
5. Determine whether you must customize the software for different parts of the company.
6. Determine how often you will have to update user templates or custom files.

There are other requirements that determine targeting specifications, such as users who have existing versions of a package or minimum hardware requirements. Special considerations for targeting include the dynamic nature of any organization and the resulting addition and removal of resources from a target set over time.

To help you assess the administrative and user requirements in your organization, see "Planning a Managed Environment" in this book. To learn how to create and then link a GPO to a site, to a domain, or to an OU, see "Designing a Group Policy Infrastructure" in this book.

Targeting Software to Users and Computers

Before you begin the process of targeting software to users and computers, you must know how to create a GPO and how to link it to a site, to a domain, or to an OU.

Group Policy is an extremely flexible tool that you can use to provide users with controlled access to the specific software that they need to do their jobs. You can use Group Policy to control various levels of software administration for users and computers in a specified site, domain, or OU.

To create GPOs for software deployment, you must find commonality across applications, users, and administration. In a simple situation, a set of users who are members of the same OU must have access to a specified set of applications that are administered by a single group of administrators. In this situation, you can put the applications in a single GPO, link that GPO to the applicable OU, and then assign or publish the applications for the group of users.

Determining the Number of Software Installation GPOs

To minimize the number of GPOs that you must have to install the software applications in the environment, it is recommended that you set the GPOs to publish a number of related applications. For example, if you determine that when users install Microsoft® Project, they typically also must have Microsoft® Visio® drawing and diagramming software. Therefore, it makes sense to combine these two applications in a single GPO. By logically grouping applications, you can reduce overall administration and management costs.

An alternative to grouping applications is to create a separate GPO for each application you want to manage by using Group Policy. By creating separate GPOs, you have more flexibility because the application of GPO's is more granular. However, the number of GPOs that are assigned to each client is higher. More GPOs leads to slower start and logon times. However, the number of settings in each GPO is the most important factor because processing each .adm file requires a set amount of time, regardless of the number of settings that the file contains.

In small organizations, it is not uncommon to see more than 100 different applications. In large multinational organizations, the number can be significantly higher. It can be difficult and time-consuming to manage all these applications by using a separate GPO for each application. However, if it ever becomes necessary to delete or disable an application installation Group Policy, deploying the applications in separate GPOs can prevent massive removals and reinstallations of the applications if the applications fall out of management scope (for example, if the client computer or user is moved to another organizational unit). Administrators must balance the benefits of this approach from the point of view of both administrators and users.

Recommendations for Creating GPOs for Software Deployment

When you create GPOs for software deployment, it is recommended that you do the following:

- Create separate GPOs for administrators, based on their roles, to simplify administrative delegations. However, these administrators must communicate with each other about the applications that they are deploying to avoid affecting each other's installations and creating unnecessary network traffic.
- Use GPOs to match applications to users and the tasks they perform.
- Assign or publish a package only once per GPO. For example, assign Office XP to the computers that are affected by a GPO, but do not assign or publish it to users who are affected by the same GPO.
- Minimize the number of GPOs that you create because the overhead for processing each GPO increases user logon time. Network performance is much better if you use a single GPO that deploys 100 applications than if you use 100 targeted GPOs. Take advantage of GPO inheritance to distribute the application throughout your organization. If necessary, use security descriptors, such as Access Control Entries on the GPO for finer control over who receives the software.



Note

The depth of OUs has very little effect on client processing time per GPO. However, a deep OU hierarchy can significantly complicate the troubleshooting process. For more information about inheritance and security descriptors, see "Designing a Group Policy Infrastructure" in this book.

- Place GPOs that assign or publish software applications as high as possible in the organizational unit structure. This makes it easy to give all users or computers in an organization access to an application. It also reduces administration because you can use a single GPO to assign or publish an application, instead of re-creating that object in multiple containers that are lower in Active Directory.
- Plan ahead for removal when you initially deploy the software. If you want the application to be removed when a GPO is no longer applicable, select the **Uninstall this application when it falls out of the scope of management** option. You can configure this option on the **Deployment** tab in the **Properties** dialog box. Right-click the managed software in Group Policy, and then click **Properties**.

- Specify application categories. When you use categories, it is easier for users to find applications in **Add or Remove Programs**. You can configure this option on the **Categories** tab in the **Properties** dialog box. Right-click the managed software in Group Policy, and then click **Properties**.



Important

Security Group filtering is not recommended because the final effect of filtering is difficult to predict before deployment or to analyze afterward. Although using this method might seem simple at first — one GPO can be used for everyone, with certain settings excepted for certain groups — it is difficult in practice.

The impact of advertisement scripts on startup and logon time

Evaluate the size of each advertisement script of every application that you assign. The size of the script can vary dramatically, from 1 kilobyte (KB) to 200 KB (typical) to 700 KB (very large application suites). Windows XP Professional advertises all assigned applications each time a user logs on. This does not generate network traffic, but it does require the client computer to process Windows Installer each time a user logs on. The first time that applications are assigned, the target must load and process the advertisement scripts for each new application. After this, each time the target user logs on, Windows Installer reprocesses the downloaded scripts for every assigned application to verify that these applications are properly configured. Typically, published applications do not affect user logon time. Therefore, it is not a problem to publish applications to a large number of users, regardless of whether they need the applications right away. The exception is when you publish an upgrade to an application that is already published or assigned. The operating system retrieves this publication data from Active Directory during the logon process. The effect this has on users is not as significant as the effect of assigning nonessential applications. It is best to assign only necessary software.

You can see the size of application management files by opening the applications folder or the scripts folder in Sysvol. These folders are located in the user folder or the computer folder of your domain controller. For example:

```
\\Server Name\Sysvol\Domain Name\Policies\GPO GUID\User\applications
```

-or-

```
\\Server Name\Sysvol\Domain Name\Policies\GPO GUID\Computer\Scripts
```



Caution

Never edit or open the files in these Sysvol folders. Doing so can damage the application scripts and affect every client in the GPO. Always perform all necessary edits by using Group Policy Object Editor.

Scaling Group Policy to Meet Your Needs

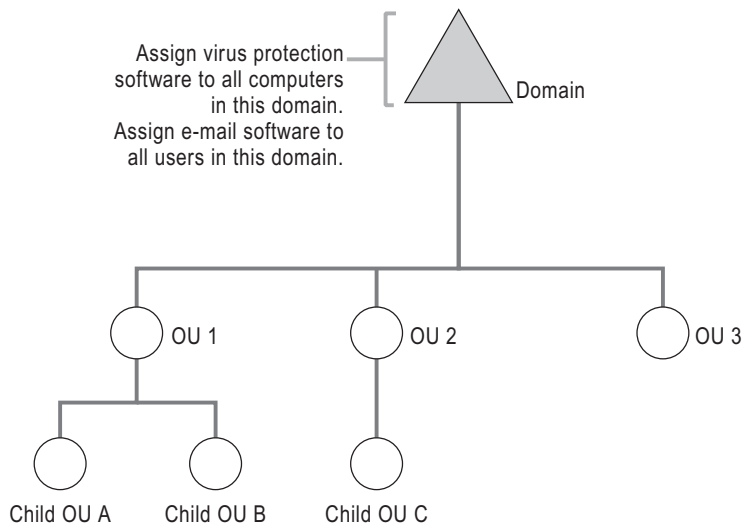
The way you use Group Policy to manage software depends on your network infrastructure, administrative hierarchy, and the business requirements of your organization. Many large organizations have a central IT administration that has delegated authorization. Others have either strictly centralized or decentralized IT groups. Regardless of how your IT administration is organized, you must communicate with software administrators at all levels of the domain hierarchy so that all software administrators know what software each other assigns, publishes, or removes at each level. The administrative tasks that other software administrators perform at other levels of the domain hierarchy can affect how you scale Group Policy to deploy and manage software at your level.

Applying Group Policy high in the domain hierarchy

When you apply Group Policy settings high in the domain structure, you can reach more users than if you apply settings at a lower OU level. You also decrease application administration for the same application. You can filter user groups lower in the Active Directory hierarchy to avoid giving all users all the applications that you deploy by using Group Policy.

If an application is assigned at the domain level, all users in the domain receive that application. Administrators at the domain level manage applications that are deployed at that level. By managing applications at the domain level, you relieve administrators in the OU levels beneath it from having to manage them.

Figure 8.5 illustrates how you can assign software to users and computers by applying GPOs at the domain level, and how that software assignment is inherited by the associated OUs by default.

Figure 8.5 Assigning Application-Based GPOs at the Domain Level**Important**

Administrators cannot control installation order. Although the Group Policy user interface displays the list of applications alphabetically, installation order is based on the order in which the applications are added to the GPO. However, you can create launch conditions in the .msi package so that a particular software package is not installed until a condition is met. For example, you might specify that a dependent package is not installed unless the application it requires to operate correctly is installed.

Targeting Software to Multinational Users

While you are planning your Group Policy deployment to meet the needs of your users, note the needs of multinational users. Multinational corporations share information and collaborate on a worldwide basis. Before Windows 2000, the operating-system support and the files generated with an application in one language were not necessarily compatible with a file that was created by the same application in a different language. However, in Windows Server 2003, you no longer have to apply, track, and maintain a different service pack and tool and application set for each localized version. You can now assign or publish the same software to every user or computer in the company, regardless of location.

Table 8.4 shows the conditions that the software installation extension of Group Policy must verify to determine whether to install an application on a computer that runs Windows 2000 or a later version of the operating system.

Table 8.4 Application Installation Conditions to Verify

Condition	State of the Package
The language for non-Unicode applications is any value and the product language is either neutral or English.	The package is either installed or advertised.
The Ignore Language parameter is set in the software installation extension of Group Policy for the managed package.	The package is either advertised or installed, whether or not the system locale and product language match.

The **Ignore Language** parameter can be configured by clicking the **Advanced** button on the **Deployment** tab, which you can open by right-clicking the managed software in Group Policy, and then selecting **Properties**.



Caution

If you deploy two versions of the same application that have different product languages (such as an English version and a German version), and they are in the same GPO, be sure to give the application a different product code for each language.

Assigning and Publishing Software

Because you can publish software for users, assign software to users, or assign software to computers, you can establish a workable combination of those three options to meet your software management goals. The following is a comparison of these methods.

Publishing software for users

Typically, after you publish a software package to users in a site, domain, or OU, the users can use **Add or Remove Programs** to install the software. An exception is when you publish an application in a new GPO, and you must simultaneously link the GPO to the users in a site, domain, or OU. If you link a GPO and deploy the software at the same time, you must refresh the Group Policy before the application appears in **Add or Remove Programs**. Additionally, the application can be installed by opening an associated document if the application is deployed to do that (if **Auto-Install** is selected).

The user can remove the software, and then later choose to reinstall it, by using **Add or Remove Programs**.

Assigning software to users

There are three methods for assigning software: assign to users on-demand, assign to users, or assign to computers.



Important

Check software license agreements before you assign applications to users because assigning software can result in an application being installed on multiple computers. Issues might occur, regardless of whether you use the policy setting option **Remove the application if it falls out of the scope of management**.

Assigning software to be available on demand After you assign a software package to users in a site, domain, or OU, the software is advertised on the desktop. The application becomes available to the user the next time the user logs on (if application's GPO applies to that user). The application is fully installed by the user from the **Start** menu, from **Add or Remove Programs**, from a desktop shortcut, or by opening a document (on demand) that has a file name extension that is associated with the application.

The user can remove the software, and then later choose to reinstall it as they did previously. By using Group Policy, you make sure that assigned applications that are available on-demand are available, regardless of whether users remove them, and that the applications are available again the next time the user logs on or starts the computer.

Assigning software to users After you assign a software package to users in a site, domain, or OU, you can use the **Install this application at logon** option to install the whole application the next time the computer starts, or after the user logs off and then logs on again. The application is also immediately available in **Add or Remove Programs**.

The user can remove the software, and then later choose to reinstall it as they did previously.

**Note**

Some applications that you have published might not appear in **Add or Remove Programs** in a domain that has multiple domain controllers until the changes have replicated to all domain controllers in the domain.

Assigning software to computers After you assign a software package to computers in a site, domain, or OU, the software is installed the next time the computer restarts or the user logs on.

Only the local or network administrator can remove the software, though a user can repair the software.

**Caution**

To avoid installation errors and reduce network traffic, do not assign or publish a Windows Installer package more than once in the same GPO.

Assigning Software to Users and Computers

Assign software to users or computers for either of the following reasons:

- To make a particular application available to all users of one computer, assign that application to the computer.
- To make mission-critical software available to users or computers at all times, assign the application to the users or computers.

**Note**

If you assign many applications instead of publishing them, you can cause congestion between client computers and the software distribution point servers. Use DFS to distribute the server load among multiple servers.

Assigning standard software

Typically, packages that you assign to users or computers are essential. Therefore, the applications on your standard software list are good candidates for assignment to users or computers. The easiest method for assigning standard software to a large number of users in your organization is to apply the GPO at the highest level of the domain hierarchy, as shown in the following example.

Assigning Software to Computers and Users Example

It is standard for all users at a corporation to receive virus-protection software and e-mail. The software administrator creates two GPOs and assigns the two software packages. She assigns the virus protection software to all computers, and the e-mail application to all users. After the GPOs are created, she applies the GPOs at the domain level of the Active Directory structure so that all members in the domain receive the software assignments.

It is recommended that you assign virus-scanning software to all computers in the organization because this software must function for every user of each computer. Some organizations consider e-mail application to be mission-critical, but some e-mail packages are very large. Installing large packages over an already congested or slow network link can negatively affect network bandwidth. If this is not an issue for you, and you want all users to have e-mail, you can assign the e-mail package to everyone in the organization. After you configure software assignment in the appropriate GPO, apply the GPO that is associated with standard software applications to the root domain.

► To prepare for assignment of software to users and computers

1. Determine the size of each application. Very large applications might not be appropriate for automatic installation. For example, a product such as Office 2000 can take a long time to install. Make sure that your deployment plan includes an analysis of how much traffic your network can handle.
2. Assign applications only to the users who require them.
3. Determine whether you can include some of the common applications in a Remote Installation Protocol preparation (RIPrep) image, or other automated image technology. RIPrep can reduce software installation time during the logon process or at initial selection of the application. RIPrep and Remote Installation Services (RIS) are excellent methods for creating these images. For more information about RIPrep and RIS, see “Designing RIS Installations” in *Automating and Customizing Installations* of this kit.

Configuring a complete application Installation

When you assign an application to a user, you have the option to install the whole application the first time the user logs on after deployment, or you can configure to install the application on demand. You can select the **auto-install by file activation** option on the **Deployment** tab in the **Properties** dialog box. Right-click the managed software in Group Policy, and then click **Properties**.

You can configure the installation to occur the first time the user logs on after deployment. This method ensures that the user has the whole application available when it is needed. However, this method also requires a longer logon time while the application is being installed. Without this method, a portable-computer user who is not connected to the network might discover that an essential feature is not available. By using this method, you provide a less confusing experience for users who might think that an application is installed, only to find that clicking the shortcut triggers an installation.

For applications that you can customize, such as Office XP, you can make all components of the application available at installation. This approach to installation is a Windows Installer authoring function, not a Group Policy software deployment function. For example, the author of the installation package can select to make features such as a spelling checker available on first installation. This increases the installation time somewhat, but it also provides all needed features on first use. Performing a complete application installation is a good method to use for mobile users who are not connected to the network most of the time. When the user requires the spelling checker, it is already installed on the computer.



Note

By default, Group Policy allows you to configure a user-assigned application that has a staggered, on-demand installation. By using Windows Server 2003, you can turn off the default installation and install the entire application at once. This mirrors the behavior of computer-assigned application installation.

Enabling users to install applications and features on demand

When you configure Group Policy so that users can install only the features (such as the spelling checker) or components of a product as they use them, you avoid wasting client disk space to store features that users do not need or use. Additionally, this method helps to prevent network congestion that is caused by users downloading large applications. The core application is not installed until the user activates the application on the computer by one of three ways: selecting the application from the **Start** menu, clicking a shortcut on the **Desktop**, or by activating a document of a file type that is associated with the application. After the core application is installed, the user can install features of the product as needed.

The following installation process is typical for user-assigned applications intended for on-demand applications:

1. The user logs on to a computer running Windows 2000 (or a later version of the operating system).
2. The application management service process advertises applications on the user's desktop or on the **Start** menu.
3. The user invokes the needed software from either the **Desktop** or the **Start** menu, or by selecting a file that has a file name extension for an assigned application. This action starts Windows Installer.
4. Windows Installer installs the requested Windows Installer package from the distribution point.
5. Windows Explorer starts the application.

Publishing Software for Users

The benefit of publishing software, instead of assigning it, is that it requires less management when change occurs in the Active Directory structure. Typically, you publish applications that are nonessential for the users. When you publish software for a user, it does not initially appear to be installed on the computer. There is no Windows Installer advertisement information about the software on the computer in the registry, on the desktop, or on **Start** menu as a shortcut. On an as-needed basis, the user installs the published software by using **Add or Remove Programs** in **Control Panel**. Users can also install the published application by selecting a file that has a file name extension for an application.

► To publish software for users in your organization

1. Determine the size of each application. Some products take a long time to install, so consider if it is more appropriate to assign the application, instead.
2. Determine whether you can publish certain applications to all users (without restriction) in your administrative area.
3. Create a table of applications. This table includes the locations from which users can install the application files.
4. Publish all .zap files. You cannot assign .zap files.

When you publish applications, users do not need to remember server share names or locations for installing software. In Windows XP and Windows Server 2003, when a user clicks **Add or Remove Programs** in Control Panel, and then clicks **Add New Programs**, a list appears that provides available software categories. In these specific categories, the user can see a list of the software that is published for that user name. Users can install only the software you have published for them.



Note

Because users might be accustomed to installing software from a designated share on your network, it is important that you educate users about installing and removing published software by using **Add or Remove Programs** in Control Panel.

For more information about using **Add or Remove Programs** to install software on a client computer, see “Making Software Available to Users and Computers” later in this chapter. For more information about creating software categories, see “Categorizing Applications” later in this chapter.



Note

Files that have a .zap file name extension can only be published in **Add or Remove Programs**.

After the user installs a published application, it behaves like an assigned application until the user removes the application by using **Add or Remove Programs**, or until the software administrator removes the application.

Publishing an Application Example

Employees of an organization use a custom application that includes a corporate organizational chart and an employee locator map. This application is not essential to everyone because it does not directly affect the job they perform at the company. However, employees can save time locating coworkers by using the application. Therefore, most employees will use it occasionally.

The software administrators decided to publish this application for all users and to apply the GPO at the highest level of the domain hierarchy. A user who wants to gain access to this application can install it by using **Add or Remove Programs** in Control Panel.

Publishing Software for Large and Small Groups of Users

If you have a lightly managed IT environment, you can publish an application to all users at the domain-level without restriction, and then specify a category for the application, such as Sales. In this situation, you can expect users in the Sales department to install the software in the Sales category. However, this does not prevent unauthorized users from installing the software from the Sales category.

To prevent users from installing certain software, you can either assign software to the targets that need it instead of publishing it, or you can create different GPOs. You can also turn on loopback processing, a Group Policy setting that allows you to configure user-based policy settings in a GPO so that those settings are applied regardless of who logs on to the computer. For more information about using loopback processing, see “Designing a Group Policy Infrastructure” in this book.

To publish an application to smaller groups at lower levels of the domain infrastructure, plan for more administrative management than for small groups of users at a higher level. This kind of fine-tuning requires more GPOs or filtering.

Categorizing Applications

You can organize assigned and published applications in logical categories to make it easier for users to locate the applications that they need in **Add or Remove Programs**. Use the software installation extension of Group Policy to create and modify categories of software that you want to appear in **Add or Remove Programs**. If you have a lot of software to manage, make sure that users can easily locate the applications that they need to install by creating categories that define your organizational structure, job functions, and type of software.



Note

Windows Server 2003 does not provide predefined software categories. You must define any categories that you want.

When you create software categories, do the following:

Reflect your organizational structure For example, when users in a department use a common set of applications, you can create a category named “Finance,” which includes accounting applications such as Excel and Microsoft® Access.

Reflect job functions For example, you can create a category named “Project Managers,” which includes applications such as Project and Excel.

Classify applications by the type of software For example, a category named “Presentation Tools” might include graphics programs that your organization supports, such as Microsoft® Publisher and PowerPoint.

You can also define broad categories, such as line-of-business tools or site-licensed applications.

The categories that you establish are per domain, not per GPO. You need to define them only once for the whole domain. Only users to whom you have assigned or published software can see or install the categories containing that software. To avoid creating duplicate categories, allow only one administrator to define categories for the entire organization.

Creating Categories Example

A software administrator at an organization created the Finance category for users in the Finance department. Only the users in Finance can view and install applications in this category because they are members of the GPO for which those applications are published. Correspondingly, the users in the Finance OU cannot view or install applications from the Administration, Sales, or Shipping categories because they are not members of the GPO for which those applications are published.

Conducting a Pilot for Software Deployment

Whether you assign or publish software, you need to conduct a pilot deployment using a small group of users to test and evaluates the software before you deploy it to the rest of the organization.

You can manage a software evaluation in any of the following ways:

- Evaluate the software outside the corporate environment. For example, set up a laboratory or test network environment.
- Create a GPO to manage the evaluation, and then assign or publish the software to users who are managed by that GPO.
- Edit the security settings on an existing GPO, or on the assigned or published package, to control who can install the package for evaluation.
- Manage the state of the software by switching any of the variables, such as assigned or published, visible or hidden, or auto-install set or not set. You can manage these parameters for each package by using the property pages of the software installation extension of the Group Policy Object Editor snap-in.

Deploying Software for Users

Although a single solution cannot fit all situations, the following situations illustrate commonalities that you are likely to encounter during a pilot that includes user who have different needs.

Stationary workers

In most organizations, users have their own computers and stay in one location. Typically the computers they use are desktop computers that have a consistent, high-speed connection to the network.

Typically, administrators make these clients their base model and define a standard operating environment. This environment includes standards for how to install and configure the operating system and how to use Group Policy to further configure and manage the environment. This environment also determines the software that is needed.

If these computers have the necessary hardware to use the Remote Installation Services (RIS) feature of Windows Server 2003, the administrator can include the necessary software with the operating system image. The software is then copied to the computer that runs the operating system.

For computers that do not have the necessary hardware to use Remote Installation Services, you can use the software installation extension of Group Policy to assign software to the computers. Do this by editing the GPO that manages the computers, and by using the software installation extension in **Computer Configuration** of the Group Policy namespace.

Roaming users

In many organizations, some users move or *roam* from one location to another. It is important to understand that, although the roaming users log on to different computers to do their jobs, these computers are typically connected by a high-speed connection or a LAN connection. Additionally, managed applications follow the roaming users to any computers they log on to. For example, when a user logs on to computer A and installs software, and then goes to another location and logs on to computer B, the user can see that the software that is installed on computer A is also installed on computer B. Any changes made to that software for the user or by the user on one computer propagate to all other computers to which the user logs on.



Note

Because Group Policy software deployment settings are not applied over a slow link by default, roaming users who connect to their organization's network by slow links might not see changes to their software. You can change this default behavior in Group Policy so that applications install over slow links. You can also change the network speed threshold that Group Policy uses to decide whether a link is considered "slow." For more information about slow links and Group Policy, see "Designing a Group Policy Infrastructure" in this book.

You can assign applications either to the users or to the computers. For example, if all roaming users of a certain type use a certain application, it makes sense to assign that application to the computers so that it is already installed on the computers that the roaming users will use. Sometimes you might have to assign the software to the users, instead. In this case, when the various roaming users log on to the computer, they see the applications that are assigned to them because the application is advertised. The application is only installed for the users who actually run the application.

Mobile users

Some users travel extensively to do their jobs. For example, sales personnel often spend more time at the offices of customers than at their own offices. Mobile users are different from roaming users in that they typically work from portable computers away from an office. Although mobile users log on to the same computer, their computers sometimes connect by a high-speed link and sometimes by a low-speed link.

One challenge in assigning applications to mobile users is that source files might not be available. Use the following recommendations if your organization has mobile users:

- When connected over a slow link, user assignment effectively behaves the same as publishing software to users. If Group Policy slow-link processing is set to the default in the user interface, the software is not installed on demand. However, users can go to **Add or Remove Programs** to install the assigned software.
- If users experience difficulty staying connected when they install software, verify that the connection speed and Group Policy settings are set appropriately. You can define the connection speed that is considered to be a slow link.
- Verify that all important software components that are defined by you for the user are installed initially. This allows a user who is not connected to the network to have access to necessary software components.

Shared computers

In many organizations, users share computers, such as bank tellers who work at different times and might use a different counter and computer each shift. In these environments, the software is often task-based. Although users change, the software does not. Also, the software might track who is logged on. You can manage these users or computers from a single GPO by grouping them appropriately, and then using the software installation extension of Group Policy to assign software to the computers by using the **Computer Configuration** of the GPO namespace. The software is then available for every user of that computer.

Note that when new software is assigned to a computer, it is installed when the computer restarts. If computers restart between shifts, the new software installation or upgrade might affect the total startup time of the computer. This increase in startup time occurs only if new software is assigned or the existing software is upgraded.

Another example where computers are shared is a computer lab or classroom where users share computers for a short period of time. This situation is different from the previous shared computer situation because each user might use the same applications as the previous user, or different applications. However, the computers do not move. In this case, using an Active Directory site to manage software makes sense, although grouping the computers into a single OU can also work.

Choose the method that gives you the correct level of control for applying Group Policy. Depending on your requirements, you might decide to assign software to the computer. This can work well if the software is written to keep user information (such as configuration information and saved files) separate from software information (such as executable files). Another way to manage this environment is to assign software so that users have access to the software that each needs for their training.



Tip

To rebuild a shared environment quickly and efficiently, use RIS.

Making Software Available to Users and Computers

You can make software available to users in Control Panel. By using **Add or Remove Programs**, users can manage software on their own computers. However, you can control what software is available to users in **Add or Remove Programs** by using Group Policy settings.

Add or Remove Programs includes an active Web link for each application, which provides users with the support information they need to install certain applications. However, you can overwrite the default link by using the software installation extension of Group Policy. The support link then corresponds to your internal product support resources.

You can also have this Web link point to a support page that includes information such as an FAQ about a specified application, a help desk article about using the application, or instructions for requesting support. This can save time for both users and help desk personnel.

Linking to an Internal Resource Example

When deploying Office, an administrator at a corporation replaced the default product support link with an internal link to the organization's product support resource. This allowed users to request assistance for an Office issue from an internal resource instead of by going outside the organization for product support.

Deploying Applications in a Managed Environment Example

The administrators at an organization use Group Policy to deploy and manage software. Each time they deploy software in their organization, they prepare the software for Windows Installer, and then they distribute, target, and install the software.

The sales personnel of the organization require two new sales-based applications: a sales database and an application for order entry. The sales personnel include outside sales representatives, inside sales representatives, sales management, and clerical sales staff. These users are dispersed across four OUs in the domain infrastructure. Each OU is named for the five sales office locations: Seattle Sales, San Jose Sales, Boston Sales, Atlanta Sales, and Dublin Sales. Each OU contains up to 150 users.

The software administrator plans to publish the two new sales applications for all sales personnel. The following is the process the software administrator follows to deploy the new sales applications. The software administrator performs the following tasks:

1. Obtains the Windows Installer Packages. The new sales software comes complete from the manufacturer with Windows Installer packages (SalesDB.msi and OrderEntry.msi). Each application is less than 50 MB.



Note

Because the author of the application provided the .msi files, the administrator did not need to reauthor or repack the software.

2. Creates a test environment in the lab to verify that the installation works as planned.
3. Places the software distribution point servers as close as possible to the users. In this case, the IT administrator uses the existing software distribution points in each of the U.S. sales offices because they are only 20 percent used. For the Dublin, Ireland, sales office, the IT administrator sets up a new software distribution point file server because none currently exists.
4. Creates the file shares on the software distribution points, and then copies the packages to the shares.
5. Uses DFS to manage the network traffic. The administrator configures DFS to manage the network traffic during software installation time because DFS offers load-sharing among servers and increases availability by distributing the same data across multiple servers. This helps balance the software installation traffic and protects against bottlenecks.
6. Creates a new GPO named Sales Personnel, specifying that these two applications be published to the members of the sales office organizational units. Before linking the GPO, the administrator runs GPMC Modeling to further test the deployment.
7. Links the GPO.
8. Breaks up the software deployment into four phases to minimize network traffic. However, the administrator does not want to create four GPOs. The deployment is performed Monday through Thursday for up to 150 users per day by using e-mail. On Monday the administrator sends half of the users in Atlanta and half of the users in Boston an e-mail message telling them that the new applications, “Sales Database” and “Order Entry,” are now available for installation under the **Sales Applications** category in **Add or Remove Programs**. The following day, the administrator contacts the other half of the users in the Atlanta and Boston sales offices. The administrator follows the same process for all sales offices until all sales personnel are informed about the new software.

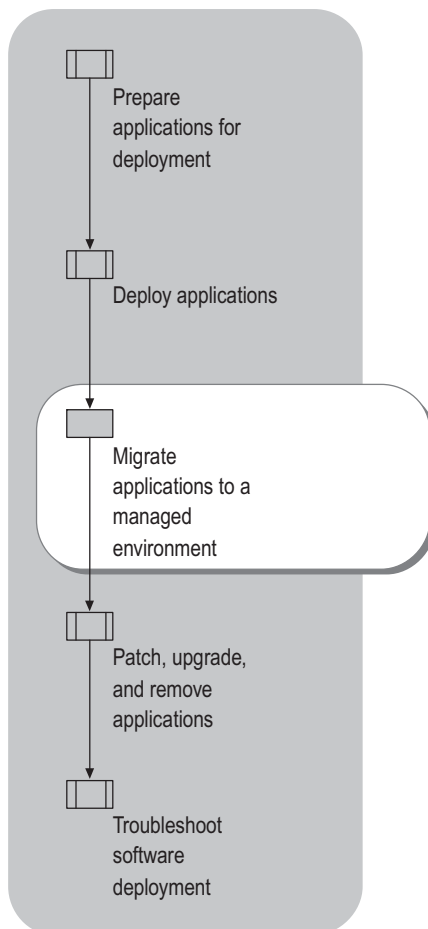
While the deployment is progressing, IT administration supports both the previously installed sales applications and the newly deployed sales applications.

After deployment, the administrator allows a grace period for users to upgrade to the new version. The administrator informs the users that the old sales database and order entry applications will expire 30 days after the new software is fully deployed. This encourages all sales personnel to install and use the new software in a timely manner.

Migrating Applications to a Managed Environment

When you decide to migrate your users and computers from an unmanaged environment to a managed environment, you must also choose a method to migrate your unmanaged applications. Figure 8.6 shows this phase in the Group Policy-based application-deployment process.

Figure 8.6 Migrating Applications Stage of Deployment



The two most common methods of migration are the following:

- Deploy applications to Windows NT 4.0 for transition to a managed Windows Server 2003 environment. Use this method if you are using a version of Windows that is earlier than Windows 2000.
- Use RIS to deploy software, and use the software installation extension of Group Policy to manage it. Use this method if you run Windows 2000 Server or Windows Server 2003. This method is recommended for deploying the operating system and standard applications to a large group of users or computers.

In either case, you can use the software installation extension of Group Policy to manage your applications.

Deploying Applications for Transition to a Managed Windows Server 2003 Environment

If you have plans to migrate to Windows Server 2003, you can deploy applications in a Windows NT 4.0 environment now, and then migrate to the Group Policy–based, managed Windows Server 2003 environment later. By planning ahead for a migration from Windows NT 4.0 to Windows 2000 Server or Windows Server 2003, you do not have to remove and reinstall applications later.

Planning for Future Migration Example

A software administrator at an organization wants to deploy Office 2000 in a Windows NT 4.0 environment. Management wants to deploy the Windows 2000 Server or Windows Server 2003 operating system, and then use Group Policy to manage Office 2000. With that in mind, the administrator anticipates moving computers that have the unmanaged Office 2000 to the managed environment. This is to make sure that the administrator will not have to remove and then reinstall Office 2000.

Use a Windows Installer package, a transform (if you must have one) for the package, and a software distribution point that is exactly the same as the Windows Installer package and transform combination that you plan to use when it is managed.

You can create the software distribution points now for use after you successfully transition to the new software.

► To make sure that the future transition is successful

1. Create the software distribution points, and then install one or more Windows Installer package and transforms in the same shared folder.
2. Install the software by using the Windows Installer with the following parameters:

```
>msiexec /I \\servername\share\<software.msi> TRANSFORMS =
\\servername\share\<software.mst> /qb
```

In this example, Software.msi is the Windows Installer package that you are installing, and Software.mst is the transform that you want applied at deployment time.

After Windows 2000 Server or Windows Server 2003 is in place, including the Active Directory and Group Policy infrastructure, you can perform the following tasks:

1. Assign the software in the appropriate GPO, using the same software distribution point, Windows Installer package, and transform.
2. Move the computer object into an Active Directory container with the associated GPO, or link the GPO to the Active Directory container with the computer object.



Important

Use the original Windows Installer package, the same transform, and the same software distribution point and shared folder when you redeploy the application in the managed environment. In this case, the software will not be removed and then reinstalled. Instead, the software installation extension of Group Policy detects that the software is the same and does only what is necessary to continue to manage the software in the new environment.

Using RIS to Deploy Software and Group Policy to Manage Applications

You can use RIS to deploy the operating systems and specific applications to client computers, and then use the software installation extension of Group Policy to manage the applications.

When an organization first acquires new computers, IT administrators spend a lot of time preparing them for the users. Many highly managed organizations format the hard drives of new computers to configuring them to their organization's standard configuration.

To save time, you can use RIS to create a customized image of a Windows XP Professional desktop on a source computer. Then you can save that desktop image to the RIS server. That image can include only the operating system, or it can be a preconfigured desktop image that includes the operating system and standard locally-installed desktop applications. You can use that preconfigured image to set up multiple desktops. You can create as many desktop images as required to meet the needs of all types of users in your organization.

You can rapidly and efficiently deploy the operating system and standard applications by using RIS, and then bring the software into a state where you can manage it by using the software installation extension of Group Policy.

For more information about using RIS to deploy software, see "Designing RIS Installations" in *Automating and Customizing Installations*.

Migrating Software to a Managed Environment Example

An organization continuously acquires new computers for new users and to replace old computers. The administrator saves valuable time by installing and customizing the operating system and standard software, which in this case includes Office XP. The administrator uses RIS to deploy the software, and then uses Group Policy to manage the applications after deployment. To accomplish this, the administrator performed the following tasks:

1. Set up and configures a RIS server.
2. Created a RIPrep image.
3. Used the Group Policy snap-in to create a GPO to manage the computers that are associated with the RIPrep image. Because this is an effort to standardize all desktops in the organization, this GPO applies to all computers in the organization.
4. Placed and sets up a software distribution point file server for Office XP.



Note

Office XP includes a native Windows Installer package (.msi). Therefore, the administrator did not have to obtain a package for this application.

1. Used the Custom Installation wizard (in Office XP) to customize Office XP based on the users' needs. This produced a transform.
2. Used Group Policy–based software deployment to assign Office XP to the computers in the organization-wide GPO.
3. Installed Windows XP Professional on a new source computer, and then configured the operating system. The source computer does not need to have the same hardware, but it must use the same Hardware Abstraction Layer (HAL) as the computers that the image is installed on.
4. Added the computer to the Active Directory container where it remains when it is deployed. This container holds the GPO that has Office XP assigned to the computer associated with it.
5. Restarted the source computer. When the computer restarted, the software that the administrator assigned to the computer (by using the software installation extension) installed.

After installing the software on the RIS server, the administrator used the RIPrep tool of RIS to build a desktop image of the source computer that has Windows XP Professional and Office XP installed, and then put this image on the RIS server.

When the image becomes available, a user who receives a new, PXE-enabled, client computer that supports the RIS server only has to connect to the network (connect a cable from the network card to the hub), connect the keyboard, the mouse, and the monitor, and turn on the computer.

The client computer locates the RIS server, and then downloads the Windows XP Professional operating system and Office XP. When the computer restarts after installing Windows XP Professional remotely, Windows Installer determines that Office XP is already installed on the computer, and then updates only the advertisement information. The advertisement update takes only a few seconds.

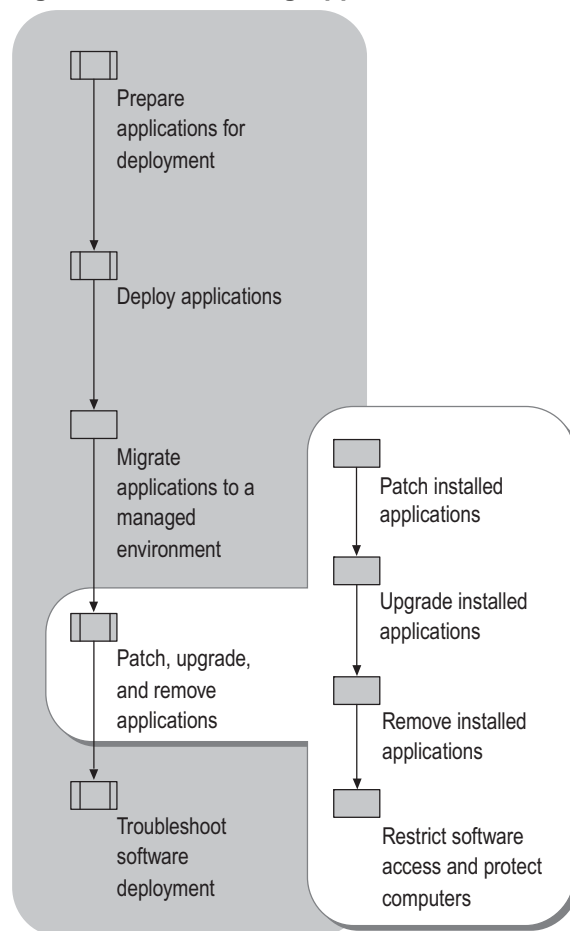
The user logs on to the computer, and then selects the first Office XP application. This causes Windows Installer to start. Although Office XP is already installed, Windows Installer properly separates the installation from the user configuration. To complete the small amount of configuration that is required for each user, Windows Installer starts each time a new user starts Office XP. This happens in Office XP regardless of whether Office XP is assigned to the user, assigned to the computer, published for the user, or installed by using of RIS.

Patching, Upgrading, and Removing Applications

The purpose of deploying patches, updates, and upgrades is similar to deploying new applications, to bring computers up-to-date. When software becomes obsolete and can no longer be updated or patched, you must remove the software.

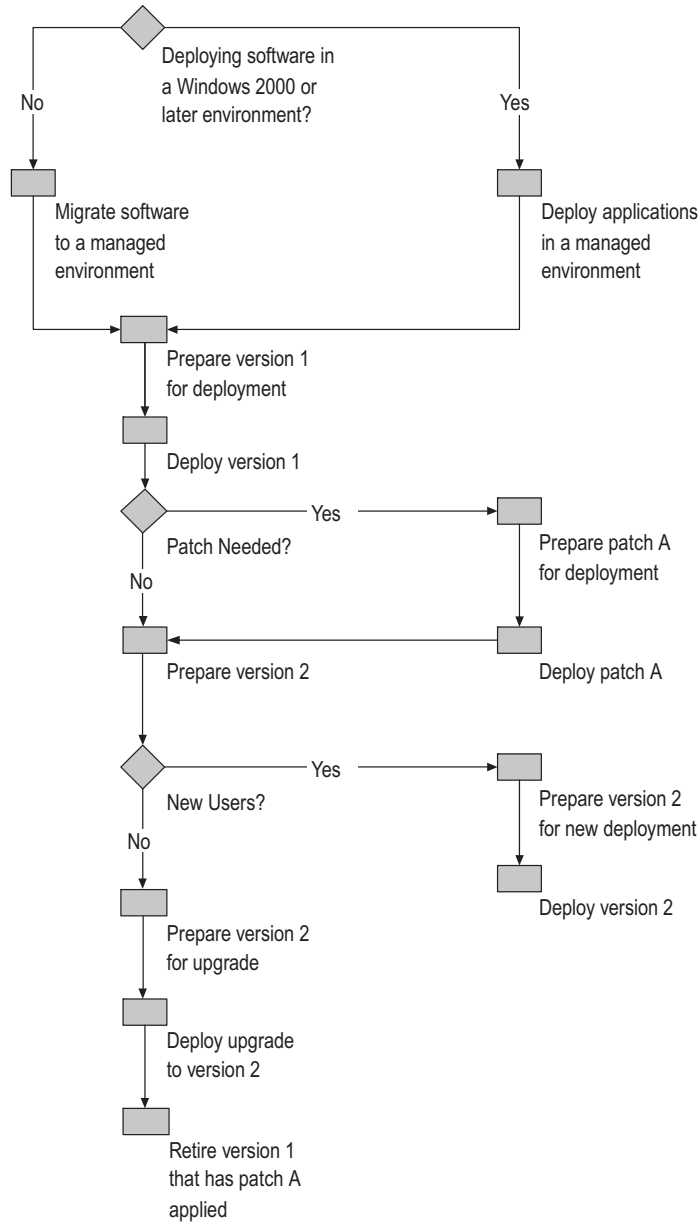
The tasks involved in maintaining software that has been deployed are described in Figure 8.7.

Figure 8.7 Maintaining Applications After Deployment



It is important to have a decision-making process for determining when to patch, upgrade to new versions of managed applications, or retire old versions. The process of deploying, patching, upgrading, and retiring is known as the *software life cycle*. Figure 8.8 illustrates a sample software life cycle.

Figure 8.8 Sample Software Life Cycle



Patching Installed Applications

Patching updates previously installed applications. You obtain patches (.msp files) from the software manufacturers or from the internal developers of the original program. You can update an existing application without removing the product. This preserves the customizations of the installation and can lower the cost of making the change. The patch might change only a few bytes of a single application file. It is more efficient to distribute those few bytes than to remove and redeploy the whole product.



Note

A patch might change all of the files and registry keys in a product.

After you apply the patch, it is cached on the user's computer, this allows the user to:

- Perform any installation on demand.
- Reinstall the application.
- Repair the application.
- Remove the application.

The patching information in this chapter applies to those organizations that have deployed software by using the software installation extension of Group Policy.

A patch package (.msp) does not include a database as a regular installation package does. Instead, it contains, at a minimum, one database transform that adds patching information to the database of its target installation .msi package. For an application to perform maintenance operations, such as adding, removing, or repairing the installation, the package codes for both the installed application and the source must match.



Important

- To remove a patch after applying it, you must remove the entire application, and then reinstall it without the patch. There is no way to roll back the changes made by a patch.
- Do not deploy a patch to an application that might add 64-bit components to a 32-bit application. This can cause failures on 32-bit clients because they cannot run the 64-bit component.

For more information about applying patches by using command-line options, see the *Distributed Services Guide* of the *Windows Server 2003 Resource Kit* (or see the *Distributed Services Guide* on the Web at <http://www.microsoft.com/reskit>).

For step-by-step instructions for patching applications, see Help and Support Center for Windows Server 2003.

Software Update Services (SUS) does not patch applications. However, you can use it in conjunction with Group Policy–based software installation. SUS is a program for managing and distributing critical Windows patches in your organization. The patches resolve known security vulnerabilities and other stability issues in Windows 2000, Windows XP, and Windows Server 2003 operating systems.

For more information about using SUS to patch and update your organization’s operating systems, see “Deploying Software Update Services” in this book.

Upgrading Installed Applications

After you determine the type of software renewal method you plan to use, Group Policy simplifies the upgrade process.

Before you update the software in your organization, you must determine which of three types of software renewal methods is appropriate for your situation:

- Small Upgrade
- Minor Upgrade
- Major Upgrade

Table 8.5 provides a quick view of the significant differences among small updates, minor upgrades, and major upgrades.

Table 8.5 Comparing Upgrade Types

Type of Renewal	Description	Product Code Property	Product Version Property
Small update	An update to one or two .msi or application files that is too small to warrant changing the product version. The package code in the Revision Number Summary Property does change. This can be shipped as a patch package or as a full product installation package.	No change	No change
Minor upgrade	A small update that makes large enough changes to warrant changing the product version, but not the product code. By changing the product version, you prevent downgrades. You also enable package sequencing. This can be shipped as a patch package or as a full-product installation package.	No change	Change
Major upgrade	A comprehensive update of the product warranting a change in the product code. Essentially, it is a new installation; optionally, it is an application removal. This can be shipped as a patch package (.msp) or as a full product installation package (.msi); only possible by using Windows Installer version 1.1 or later.	Change	Change

Small Updates and Minor Upgrades

Small updates and minor upgrades (see Table 8.6) are essentially a reinstallation that uses a new package. Regardless of the type of software renewal you choose, the .msi package code changes to make sure that the new package is used.

Table 8.6 Comparing Small Updates with Minor Upgrades

Situation	Renewal Method
A software renewal comes from the application manufacturer, and it does not include changes to the product version or product code.	A small update to the original package
A software renewal from the manufacturer changes the product version, but not the product code.	A minor upgrade to the original package

The only difference between small updates and minor upgrades is if you must differentiate between product versions.

Major Upgrades

During a major upgrade, Windows Installer searches the user's computer for applications that are related to the pending upgrade. When it locates one, Windows Installer retrieves the version of the installed application from the registry. Windows Installer then uses information in the upgrade version's database to determine whether to upgrade the installed application.

During a major upgrade, the installed version of an application might be removed, or might remain and coexist on the system with the newer version. This behavior, and its exposure to administrators, depends on the implementation of the application's setup program. For example, multiple versions of an application that are installed on the same computer might prevent the version that you install from functioning properly.

If any of the following conditions and application changes applies to your organization, you must perform a major upgrade:

- Coexisting installations of the original and updated products on the same computer
- A change in an .msi file name
- A change in the component code of an existing component
- An addition or removal of a component from an existing feature
- A change that causes an existing feature to become a child of an existing feature
- Removal of an existing child feature from its parent feature

You do not need to change the product code when you add a new child feature that consists entirely of new components that are added to an existing feature.

► To perform an update or upgrade

1. Provide adequate notice to the users that the software will be updated or upgraded by a specified date.
2. Obtain the Windows Installer package file.
3. Locate the software distribution point server and share where the original package resides.
4. Apply the update or upgrade to the original package.
5. Inform the users that the updated software is now available.

It is important that you support both the newly installed update or upgrade and the software that you plan to retire soon. Be sure to maintain the previous distribution point until all users have upgraded. Eventually, you must remove the retired version of the software. For information about removing outdated software, see "Patching, Upgrading, and Removing Software Examples" later in this chapter.

Upgrading Software by Using Windows Installer and Group Policy

During a minor upgrade or a major upgrade, Windows Installer searches for upgradeable products by querying the **Upgrade** table of the upgrade package. The newer version of the product is installed. If Windows Installer finds an older version of the product, it removes the old version. The author of the application's setup can choose to remove the old version, and then install the new version. The maintenance mode and removal do not trigger these actions because "remove existing versions of an application" is now automatic.

You can use the software installation extension of Group Policy to manually create upgrade relationships between the new package and the packages that the application replaces. This includes making a formal upgrade relationship between two similar products from completely different vendors. Again, you can either replace one vendor's application with another, or you can upgrade a repackaged application. Of course, it is recommended that you pilot or test an upgrade before putting it into production.

For examples of upgrades that are deployed by using the software installation extension of Group Policy, see "Patching, Upgrading, and Removing Software Examples" later in this chapter.

For a more information about configuring upgrades, and for a procedure for upgrading applications by using the software installation extension of Group Policy, see Help and Support Center for Windows Server 2003.

If you plan to deploy repackaged applications by using the software installation extension of Group Policy, you must allow extra time for unexpected situations that require you to create upgrade relationships manually or to create a script to remove unwanted files.

Manually creating upgrade relationships

The Windows Installer package for a repackaged application does not have declared upgrade relationships. You must manually create upgrade relationships. You can configure these relationships by using the software installation extension of Group Policy.

► To manually create an upgraded relationship

1. In the Software Installation section of the Group Policy object, right-click the managed software.
2. Click **Properties**.
3. On the **Upgrades** tab, specify the packages that the selected package will upgrade and the packages in the current GPO that will upgrade this package.
4. Click **Add** to select the packages.

Writing a script to remove files

During an upgrade, it might not be possible to completely remove a repackaged application. The removal of a repackaged application might leave components on the desktop, regardless of whether the component is shared or needed. You can create a script to remove the remaining files.

Removing Installed Applications

When you no longer support a software version, plan for its removal. First, be sure to give adequate notice to the software users before you remove the application.

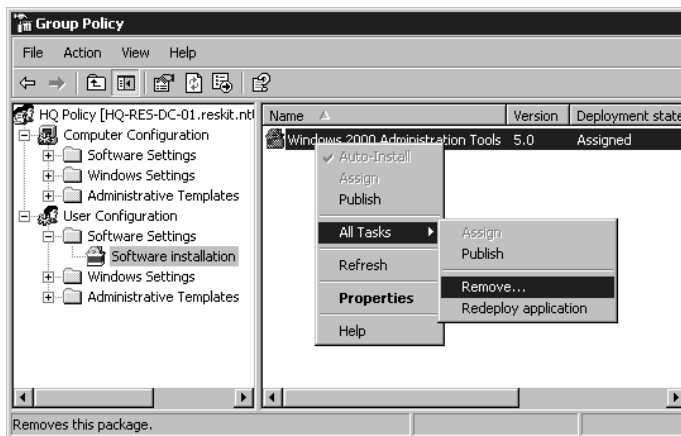
You can either force the removal of the software or make it optional, depending on, for example, whether the old software is compatible with newly deployed software. These two choices, available from the software installation extension of Group Policy, affect the removal of software.

Forced removal If the software is assigned to a computer, it is removed the next time the computer restarts. If it is assigned to a user, it is removed the next time the user logs on.

Optional removal You can stop managing the software without forcing its physical removal from the computers of users who use it. Users who currently have the software installed can continue to use it until they choose to remove it themselves.

Figure 8.9 shows how to open the **Remove Software** options menu dialog box. Right-click the software installation extension of Group Policy to view this menu.

Figure 8.9 Locating the Remove Software Option Menu



Note

To save time later, you can plan for eventual removal when you initially deploy the software. If you want the application to be removed when a GPO is no longer applicable, select the **Uninstall this application when it falls out of the scope of management** option. For more information about this option, see “Targeting Software to Users and Computers” earlier in this chapter.

See the following section for an example of removing software by using the software installation extension of Group Policy.

Restricting Software Access and Protecting Computers

Although a business might use a set of programs that it knows and trusts, and might train its administrators and Help Desk personnel to support those programs, administrators lose control as soon as users begin running unknown code. The increasing role of the Internet in business puts your network at a greater risk than ever before.

Such user-installed programs can conflict with other installed programs, change critical configuration data, or introduce a virus. Users often cannot make safe or informed choices about what software to run because viruses intentionally conceal the malicious purpose of the program. Also, the problems that are associated with running unknown code can increase support costs substantially because they lead to more system maintenance, more help desk time, and lost user productivity.

Software restriction policies, new with Windows XP and Windows Server 2003, provide a policy-driven mechanism that enables you to identify the programs that are running on computers in your domain, and to control their ability to run. By using software restriction policies, you can:

- Control what programs run on your system. For example, you can apply a rule that does not allow certain file types to run in the mail attachment directory of your e-mail program if you are concerned about users receiving viruses through e-mail.
- Run only digitally signed scripts.
- Allow users to run only specific files on multiuser computers. For example, if you have multiple users who use a single computer, you can set up software restriction policies and Access Control List settings so that users cannot make changes to computers.
- Decide who can add trusted publishers to a computer.
- Control whether software restriction policies affect all users or only certain users who use a computer.
- Prevent any files from running on a local computer. For example, if you are aware of a known virus, you can disallow a hash of that virus so that the computers in your domain cannot run that program.

A software restriction policy consists of a rule, or set of rules, that determines what programs are allowed to run, and any exceptions to the rule. Use the Group Policy Object Editor to create software restriction policies. Go to the User or Computer configuration, as appropriate. Under **Windows Settings**, click **Software Restriction Policies**. Here you can configure the parameters for **Security Levels**, set **Additional Rules**, specify **Designated File Types Properties**, and identify **Trusted Publishers Properties**.

The purpose of a rule is to identify one or more software applications, and to specify whether the application is allowed to run. Creating rules is mainly identifying software that is an exception to the default rule. You can include descriptive text with each rule to help communicate why the rule was created. A software restriction policy supports four rules to identify software.

Hash rule

A cryptographic fingerprint of the file, also called a *message digest*. When you create a hash rule for a program, Software Restriction Policies calculates a hash of the program, and then stores the hash securely. When a user tries to open a program, a hash of the program is compared to existing hash rules for Software Restriction Policies. The hash of a program is always the same, regardless of the location of the program on the user's computer. However, if a program is altered in any way (by applying a hotfix, for example), its hash also changes, and it no longer matches the hash in the Software Restriction Policies hash rule.

For example, you can create a hash rule, and then set the security level to **Disallowed** to prevent users from running a certain file. A file can be renamed or moved to another folder and still result in the same hash. However, if any changes are made to the file itself, they also change its hash value and allow it to bypass restrictions.

Certificate rule

A software publisher certificate used to digitally sign a file. For example, a company can require that all scripts and Microsoft® ActiveX® controls be signed with a particular set of publisher certificates. Certificates that are used in a certificate rule can be issued from a commercial Certificate Authority (CA) such as VeriSign, a Windows 2000 or Windows Server 2003 public key infrastructure (PKI), or by a self-signed certificate. Certificate rules are a strong means to identify software because the certificate matches the files, regardless of name or location, by using signed hashes that are contained in the signature of the signed file.

Path rule

The local or universal naming convention (UNC) path to where the file is stored. Path rules can include the following:

- Environment variables. Path rules are evaluated in the client environment. Therefore, using an environment variable, such as %Windir%, allows a rule to adapt to a user's environment.
- Wildcard characters such as asterisk (*) or question mark (?). By including a wildcard character, a rule can match all files of the specified type. For example, a rule such as *.vbs matches all Microsoft® Visual Basic® script files.

- Registry paths. You can create a path rule that looks up these registry keys for applications that store paths to their installation folders or application directories in the system registry. The registry path is formatted as follows:

%[Registry Subtree (Hive) Name][Registry Key Name][Registry Entry (Value) Name]%



Note

A registry path rule suffix cannot contain a backslash (\) character immediately following the last percent sign (%) in the rule.

The following conditions apply:

1. The registry path must be enclosed by percent signs (%).
2. The registry setting must be a **REG_SZ** or **REG_EXPAND_SZ** type. If the registry value contains environment variables, these will be expanded when the policy is evaluated.
3. Do not use HKLM as an abbreviation for **HKEY_LOCAL_MACHINE**, or HKCU as an abbreviation for **HKEY_CURRENT_USER**.
4. A registry path rule can also include a suffix path.

For example, you can use:

%HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache%OLK*



Note

When you set a path rule, verify the Access Control List (ACL) entries on the path. If users have Write access to a path, they can modify its contents. For example, if you allow Write access to C:\Program Files, any power user on the computer can copy software to the Program Files folder.

Zone rule

An Internet zone rule identifies software by the Microsoft® Internet Explorer zone from which it is downloaded. These zones are: Internet, Intranet, Restricted Sites, Trusted Sites, and My Computer. This rule applies only to Windows Installer (.msi) packages. It does not apply to software that is downloaded by using Internet Explorer.

When a user tries to install a piece of code, Windows Installer queries the software restriction policy to determine the level at which the code is allowed to run. Software restriction policies integrate with the operating system and common scripting runtimes to control the running of software, not just to hide access to applications by removing them from the **Start** menu or to hide the **Run** command. Software restriction policies go beyond this by removing the common access points for software.

Essentially, software restriction policies protect against the various Trojan horse and worm viruses that propagate through e-mail and over the Internet. Software restriction policies are a powerful way to identify software so that it can be classified as **Unrestricted** or **Disallowed**. After you identify programs, you can apply a policy to either restrict the software or to let it run.

Table 8.7 shows some recommended situations for applying available software restriction policy rules.

Table 8.7 Situations for Applying Each Rule

Sample Task	Situation to Apply Rule
Allow or disallow a specific version of a program.	Hash rule Browse to file to create hash.
Identify a program that is always installed in the same place.	Path rule with environment variables %Program Files%\Internet Explorer\iexplore.exe
Identify an anti-virus program that can be installed anywhere on a client computer.	Registry path rule %HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\InoculateIT\6.0\Path\HOME%
Identify a set of scripts on the central server.	Path rule \\Server Name\Share Name
Identify a set of scripts on a set of servers named DC01, DC02, and DC03.	Path rule with wildcards \\DC??\Share Name
Disallow all .vbs files except those in a login script directory.	Path rule with wildcards *.VBS set to Disallowed \\LOGIN_SRV\Share Name*.VBS set to Unrestricted
Disallow a file that is installed by a virus that is always named Flcss.exe.	Path rule Flcss.exe set to Disallowed
Identify a set of scripts that can be run anywhere.	Certificate rule <Certificate used to digitally sign the scripts>
Allow software to be installed from trusted Internet zone sites.	Internet zone rule Trusted Sites set to Unrestricted

The following guidelines can help you use software restriction policies effectively:

Create a separate GPO for software restriction policies When you create a separate GPO for your software restriction policy settings, you can turn them off in an emergency without affecting the rest of your security or other settings.

Never modify the default domain policy When you do not edit the default domain policy, you can always reapply it.

Never link to a software restriction policy in another domain Linking to a GPO in another domain can result in poor performance, or it might not work at all. This is true for any GPO, not just for software restriction policies in a GPO.

Test your software restriction policy first Typographical errors in rules can result in a software restriction policy that does not perform as you expect. Be sure to test your policy on a test computer first.

Turn off a software restriction policy while editing it When you edit a software restriction policy, each change you make updates the GPO. If a computer tries to synchronize Group Policy settings during an editing session, the user might receive the software restriction policy before you finish editing it. If this happens, the user's computer might be adversely affected.

Verify that trusted virus scanners are not restricted Most antivirus software has a real-time scanner program that starts when the user logs in. This program scans all files that are accessible by the user to locate possible virus contamination. Make sure that your rules allow your virus-scanning programs to run. Software restriction policies are not a replacement for antivirus software.

Filter user policies based on membership in security groups You can decide which users do not have a Group Policy object applied to them by denying them the **Apply Group Policy** or **Read** permissions on that policy. You require both of these permissions to apply Group Policy.

Use software restriction policies in conjunction with access control settings Prepare carefully if using Disallowed as the default setting. Many applications start other applications to perform certain tasks. Verify that all major tasks in your applications are covered by your rules. If your computer needs to run logon scripts, make sure that you have created a path rule that allows them to run.

Restart in Safe Mode if you experience problems with applied policies Software restriction policies do not apply in Safe Mode. If you accidentally lock down a workstation by applying software restriction policies, restart in Safe Mode, log on as a local administrator, modify the policy, run Gpupdate.exe, restart the computer, and then log on the usual way.

Always test policy on a test computer before applying it to any other computers Do not apply rules at the **Disallow** level without the proper testing. Restrictions on certain files can seriously affect the operation of your computer or network.

Rules are evaluated in a specific order. If two rules are similar or conflict, the more restrictive rule takes precedence, and the rules that more specifically match a program take precedence over rules that loosely match a program. In the case of multiple matching path rules, the most specific matching rule takes precedence. Because each rule has an associated GUID, two identical rules have two GUIDs.



Note

Environment variables are not protected by Discretionary Access Control Lists (DACLs). Therefore, if users can start a command prompt, they can redefine an environment variable to a path of their choosing.

The overall rule precedence is as follows:

1. Hash rule
2. Certificate rule
3. Path rule
4. Internet zone rule
5. Default rule

When multiple path rules match, the most specific matching rule has precedence. The following is a set of paths, listed from highest precedence (a more specific match) to lowest precedence (a more general match):

- Drive:\Folder1\Folder2\FileName.Extension
- Drive:\Folder1\Folder2*.Extension
- *.Extension
- Drive:\Folder1\Folder2\
- Drive:\Folder1\

Patching, Upgrading, and Removing Software Examples

An essential part of the software life cycle involves patching, updating, upgrading, and removing software. This section describes how to use Group Policy–based software deployment to simplify managing this life cycle.

Patching an Installed Application Example

The address of corporate headquarters for the organization has changed and the software administrators want to deploy a Microsoft® Word version 2002 fax and letterhead template patch to replace the previous fax and letterhead template files. Except for the sales offices, the OU structure is designed around the organization's departmental structure. With this in mind, the IT administrator must selectively deploy the fax and letterhead templates to the departmental OUs and the Seattle-based sales office. The sales offices in San Jose, Boston, and Atlanta do not need to receive the patch. The administrator performed the following tasks to patch some previously deployed, computer-assigned software:

1. Copied the patched (.msp) file to the applicable software distribution points. This replaced only the previously deployed fax and letterhead files for Word 2002 on each file server.
2. Opened the software installation extension in the GPO. The GPO includes the software installation extension that contains the application deployment properties of Word 2002.
3. Applied the patch to the source image by running `msiexec /a <package.msi> /p <patch.msp>`.

4. Redeployed the fax and letterhead files. In the GPO, the administrator right-clicked **Word 2002**, selected **All Tasks**, and then selected **Redeploy Application** from the available menu.
5. Prompted users by e-mail to restart their computers to make the computers recognize the patched software. After the users restarted their computers, the GPO applied the patched file, and the users had access to the new fax and letterhead templates.

Performing an In-Place Upgrade Example

For years, everyone at the organization has used a custom application specific to company business. This software is mission-critical for all users. Therefore, it will continue to be assigned to everyone in the organization. Recently, the company recruited developers to rewrite the application to include a Windows Installer package. The software administrator wants to deploy the new .msi package, and has chosen to perform an in-place upgrade. The administrator used the following process to upgrade the software:

1. Copied the new .msi package upgrade to the software distribution points.
2. Created a GPO that published the new software to all users.
3. Advised all users to update their software by the established date, with a reasonable grace period to accomplish the task.
4. After verifying that all users had upgraded, changed the software installation configuration in the GPO to assign the new version to all users.
5. Sent e-mail prompting the users to restart their computers.

After the users restarted their computers, the new Group Policy setting applied, and the users had access to the new custom application.

Performing an Upgrade to Remove and Replace Software Example

The organization signed a global licensing agreement with a new antivirus software provider. Until then, all computers in the organization had *X* antivirus software installed. By using the software installation extension of Group Policy, IT administrators safely replaced *X* antivirus software with *Y* antivirus software.

Antivirus software is critical to any network operating environment. Therefore, IT administrators assigned *Y* antivirus software to all computers in the organization. The IT administrator used the following process to replace *X* antivirus software with *Y* antivirus software:

1. Opened the software installation extension in the GPO. The software installation extension contained the application deployment properties of both *X* antivirus software and *Y* antivirus software.
2. Created an upgrade relationship between *X* antivirus software and *Y* antivirus software. On the Upgrade tab of the *Y* antivirus software Properties, the administrator selected the Required upgrade for existing packages check box. This makes all users of *X* antivirus software receive the upgrade to *Y* antivirus software.
3. Sent e-mail to prompt users to restart their computers.

After the users restarted their computers, the computers recognized the new *Y* antivirus software.

Removing Software Example

The organization terminated a site license agreement with a certain software distributor for a marketing application that was previously published to users in the Marketing department. Software administrators of the organization needed to verify the removal of all copies of the unlicensed software. The software administrator used the following procedure to remove the unlicensed software in a GPO:

1. Opened the software installation extension in the GPO, which included the deployment properties of the application to be removed.
2. Right-clicked the application that the administrator wanted to remove.
3. Selected **All Tasks**, and then selected **Remove**.
4. In the **Remove** dialog box, selected the **Immediately Uninstall** check box.

After completing the removal procedure, the administrator did not prompt users to restart their computers. Instead, users were allowed to restart their computers at various times, in the course of their own work routines. That approach naturally reduced network load. However, use care at peak times, such as Monday mornings, when many people arrive at work at the same time. If the software is assigned to the users, their typical log off and log on process performs the same function.

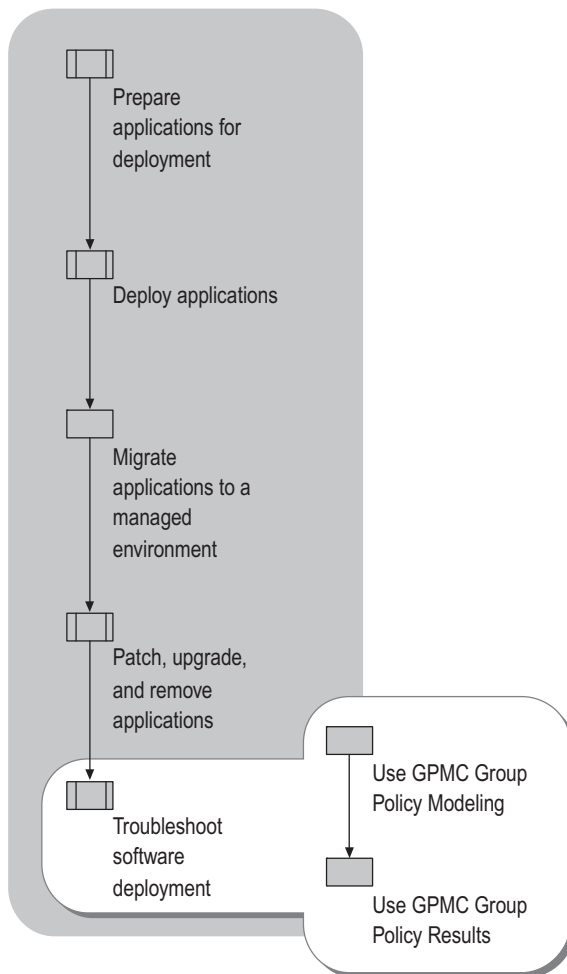
After the users restarted their computers, the GPO was applied, and the users no longer had access to the unlicensed software.

Troubleshooting Software Deployment

The new Group Policy management snap-in (GPMC) provides tools for preventing and resolving Group Policy–based software installation issues. Also, Microsoft® Windows® Server 2003, Standard Edition includes command-line RSoP tools that you can use to prevent and troubleshoot problems that might occur when you deploy Group Policy–based software (process indicated in Figure 8.10). GPMC and RSoP help you to do the following:

- Assess how Group Policy affects software deployment, updates, and removal.
- Identify and diagnose Group Policy setting failures.
- Prevent conflicts among applications that share components.
- Protect computers from unknown or infected code.
- GPMC also provides printable HTML reports for modeling your Group Policy design before deployment, and for logging its results after deployment.

Figure 8.10 Using GPMC to Troubleshoot Your Application Deployment



To prevent problems, use the Group Policy Modeling feature of GPMC to determine how software deployment, update, and removal configurations affect a target group of users and computers before you deploy, update, or remove software. To troubleshoot post-deployment problems, use the Group Policy Results feature of GPMC to see what Group Policy settings are actually in effect for a user or computer.

For more information about using GPMC to prevent and resolve Group Policy deployment issues, see “Designing a Group Policy Infrastructure” in this book. For complete step-by-step information about using GPMC, see GPMC online Help.

Using GPMC Group Policy Modeling to Evaluate Group Policy Settings Before Deployment

Use Group Policy Modeling to calculate the net effect of several GPOs before deployment. These calculated settings are reported in HTML and are displayed in a GPMC browser window on the **Settings** tab in the **Details** pane for the selected GPO. You can expand and contract the settings under each item by clicking **hide** or **show** so that you can see all the settings, or only a few. To create a Group Policy Modeling query, you must have the **Perform Group Policy Modeling analyses** permission on the domain or OU that contains the objects on which you want to run the query.

To run the wizard, right-click **Group Policy Modeling** (or an Active Directory container), and then click **Group Policy Modeling Wizard**. If you run the wizard from an Active Directory container, the wizard fills in the **Container** fields for user and computer with the LDAP distinguished name of that container.

When you have answered all the questions in the wizard, your answers are saved as a query that is represented by a new item under the **Group Policy Modeling** item. Your answers appear as if they were from a single GPO. However, the display does show which GPO is responsible for each setting, under the heading **Winning GPO**.

To save the results of the modeling, right-click the query, and then click **Save Report**. You can also print the results by right-clicking the query, and then clicking **Print**.

Using GPMC Group Policy Results to Evaluate Group Policy Settings After Deployment

Use Group Policy Results to see what Group Policy settings are actually in effect for a user or computer. Use this GPMC feature in your staging environment before you deploy managed software in your production environment. The settings are reported in HTML and appear in a GPMC browser window on the **Settings** tab in the **Details** pane for the selected GPO. You can expand and contract the settings under each item by clicking **hide** or **show** so that you can see all the settings, or only a few. To access Group Policy Results data for a user or computer, you must have the **Remotely access Group Policy Results data** permission on the domain or organizational unit that contains the user or computer, or you must be a member of a local Administrator's group on the appropriate computer.

To run the wizard, right-click **Group Policy Results**, and then click **Group Policy Results Wizard**.

When you have answered all the questions in the wizard, your answers are saved as a query that is represented by a new item under the **Group Policy Results** item. Your answers appear as if they were from a single GPO. However, the display does show which GPO is responsible for each setting, under the heading **Winning GPO**.

To save the results, right-click the query, and then click **Save Report**. You can also print the results by right-clicking the query, and then clicking **Print**.

Preventing and Resolving Software Deployment Issues Examples

You can use the Group Policy Modeling feature of GPMC to prevent or resolve software deployment problems. Perhaps more importantly, you can use Software Restriction Policies to control the running of code and prevent future problems.

Example one

By using Group Policy Modeling in GPMC, an administrator simulated moving a user from one OU to another to see what effect it might have on that user. Each of these OUs had two separate GPOs applied to it. By seeing the results of the simulated move, the administrator discovered that the user's spreadsheet application had been downgraded to an earlier version. Additionally, the user no longer had access to a word processor application.

Before the actual move, the administrator of the existing OU contacted the administrator of the target OU to request that the most recent version of the spreadsheet and word processor applications be made available to the migrating user in the target OU. The target administrator did this by creating a security filter, and then making the user a member of either one or the other, and then filtering.

Example two

An administrator wanted to examine the result of deploying a software upgrade of an existing application that was assigned to a particular group of users. When the administrator ran the scenario by using Group Policy Modeling in GPMC, the following unexpected result occurred: The GPO that contained the package was not visible to users in the Sales and Marketing departments. By examining the HTML results of the Group Policy Modeling, the administrator verified that another GPO was taking precedence over the GPO that contained the new upgrade. In this case, the administrator configured the GPO that contained the new upgrade to override the GPO that was already in place.

For more information about using GPMC to prevent software deployment issues, see the *Distributed Services Guide* of the *Windows Server 2003 Resource Kit* (or see the *Distributed Services Guide* on the Web at <http://www.microsoft.com/reskit>).

Troubleshooting by Using GPMC Modeling Examples

The following situations demonstrate ways to use GPMC Modeling at the organization level.

Example one

A help desk administrator used logging mode to locate and determine the reason that a user received the wrong version of an application. The user received a less-powerful version of the required software.

The administrator used the Group Policy Modeling in GPMC to verify which version was installed. The HTML report showed that the client computer did not have the correct language version.

After diagnosing the problem, the administrator published the correct version of the application. The user could then install it by using **Add or Remove Programs**.

Example two

A sales employee from Seattle accepted a new position in the Boston Human Resources department. The standard applications that were available in Seattle were Microsoft® Exchange E-mail, Office, a sales database, and an order entry application. In Boston, the employee discovered that he did not have access to the Human Resources database, so he contacted the help desk for assistance.

The help desk administrator started Group Policy Modeling, and then viewed the software installation extension part of the HTML report. The report showed which applications appeared in **Add or Remove Programs** on the client computer. The **Origin** field in the list of available applications showed that all the applications were coming from the GPO that was linked to the Seattle OU.

Because GPOs are set at the OU level, the administrator moved the user from the Seattle OU to the Boston OU. After that, the user could install the Human Resources database by using **Add or Remove Programs**.

For more information about using GPMC for troubleshooting software deployment issues, see the *Distributed Services Guide* of the *Windows Server 2003 Resource Kit* (or see the *Distributed Services Guide* on the Web at <http://www.microsoft.com/reskit>).

Blocking a Malicious Script by Using Software Restriction Policies Example

The organization wanted to protect itself from script-based viruses. The LoveLetter virus, technically called a worm, had cost the organization considerable expense. This worm has over 80 variants. The LoveLetter worm, written in the language Visual Basic Script, appears as LOVE-LETTER-FOR-YOU.TXT.VBS.

Administrators at the organization created a software restriction policy to block this worm from running by explicitly blocking LOVE-LETTER-FOR-YOU.TXT.VBS. They used a hash rule to prevent this script from running regardless of whether the file name changed. In the past, the organization had used VB Script files for systems management and logon scripts. By blocking all .vbs files from running, they would have protected the organization. However, they also would have penalized it because users could not have use VB Scripts for legitimate purposes.

For information about how to obtain a certificate and digitally sign files to increase the level of security in your environment, see Help and Support Center for Windows Server 2003.

Additional Resources

These resources contain additional information and tools related to this chapter.

Related Information

- “Choosing Your Automated Installation Method” in the *Automating and Customizing Installations Guide* in this kit, for more information about deploying and installing operating systems.
- “Designing a Group Policy Infrastructure” in this book.
- The *Distributed Services Guide* of the *Windows Server 2003 Resource Kit* (or see the *Distributed Services Guide* on the Web at <http://www.microsoft.com/reskit>) for more information about Active Directory, Group Policy, and Windows Installer.
- *Designing and Deploying Directory and Security Services* of this kit for more information about Active Directory.
- “Designing RIS Installations” in *Automating and Customizing Installations* of this kit for more information about Remote Installation Services.
- “Planning Deployments” in *Microsoft® Windows® XP Professional Resource Kit Documentation* (or see “Planning Deployments” on the Web at <http://www.microsoft.com/reskit>).
- “Designing the Active Directory Logical Structure,” in *Designing and Deploying Directory and Security Services* of this kit.
- “Designing and Deploying File Servers” in *Planning Server Deployments* of this kit.
- “Part 2: Deploying Distributed Security Services” in *Designing and Deploying Directory and Security Services* of this kit.
- “Planning a Secure Environment” in *Designing and Deploying Directory and Security Services* of this kit.
- *Microsoft® Systems Management Server Administrator’s Guide* for more information about SMS.
- The Group Policy Management Console link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources> for a free download of GPMC.
- The Microsoft Systems Management Server link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.
- Windows Installer Software Development Kit (SDK) link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Related Tools

- Group Policy Management console (GPMC).
The all-in-one Group Policy management tool. For a free download, see the Group Policy Management Console link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Related Job Aids

- “Worksheet A.42 Assessing Software Management Tasks” (DMEUSE.42.doc) on the *Microsoft® Windows® Server 2003 Deployment Kit* companion CD (or see “Worksheet A.42 Assessing Software Management Tasks” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.43 Packaging Software” (DMEUSE.43.doc) on the *Windows® Server 2003 Deployment Kit* companion CD (or see “Worksheet A.43 Packaging Software” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.44 Preparing Your Network for Deploying Applications” (DMEUSE_44.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.44 Preparing Your Network for Deploying Applications” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.45 Identifying Performance Issues Between Client Computers and Software Distribution Point Servers” (DMEUSE_45.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.45 Identifying Performance Issues Between Client Computers and Software Distribution Point Servers” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.46 Evaluating Strategies for Connecting Remote Users” (DMEUSE_46.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.46 Evaluating Strategies for Connecting Remote Users” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.47 Assessing Administrative Requirements and Business Needs of the Users in Your Organization” (DMEUSE_47.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.47 Assessing Administrative Requirements and Business Needs of the Users in Your Organization” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.48 Assigning and Publishing Software” (DMEUSE_48.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.48 Assigning and Publishing Software” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.49 Using GPO Back Up Log Sheet” (DMEUSE_49.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.49 Using GPO Back Up Log Sheet” on the Web at <http://www.microsoft.com/reskit>).

- “Worksheet A.50 Distributing Software Using Group Policy” (DMEUSE_50.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.50 Distributing Software Using Group Policy” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.51 Targeting Software to Multilingual Users” (DMEUSE_51.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.51 Targeting Software to Multilingual Users” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.52 Creating a Pilot Plan for Software Installation” (DMEUSE_52.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.52 Creating a Pilot Plan for Software Installation” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.53 Identifying Software Installation Issues” (DMEUSE_53.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.53 Identifying Software Installation Issues” on the Web at <http://www.microsoft.com/reskit>).
- “Worksheet A.54 Identifying Software Maintenance Issues” (DMEUSE_54.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Worksheet A.54 Identifying Software Maintenance Issues” on the Web at <http://www.microsoft.com/reskit>).

Deploying a Simple Managed Environment



Microsoft® IntelliMirror® management technologies and Group Policy combine the advantages of centralized computing with the performance and flexibility of distributed computing. This chapter incorporates the use of these technologies, described throughout this book, in a cohesive plan for creating a simple managed environment.

In This Chapter

Overview of Deploying a Simple Managed Environment	430
Deploying the Network Infrastructure	435
Deploying the Logical Infrastructure	447
Preparing Shared Folders	452
Installing Software	458
Setting Policies to Manage User Data and Settings	462
Testing and Deploying Your Configuration	470
Additional Resources	478

Related Information

- For more information about how to use IntelliMirror technologies to create a managed environment, see “Planning a Managed Environment” in this book.
- For more information about Group Policy, see “Designing a Group Policy Infrastructure” in this book.
- For more information about user profiles, folder redirection, disk quotas, and offline files, see “Implementing User State Management” in this book.
- For more information about using Group Policy to deploy application software to your users, see “Deploying a Managed Software Environment” in this book.

Overview of Deploying a Simple Managed Environment

This chapter provides a blueprint for deploying a simple managed environment. While it provides a complete end-to-end management solution for a small computing network, larger organizations can also use this chapter as a starting point for their configuration, and scale out as needed.

You can leverage the information in this chapter in two ways.

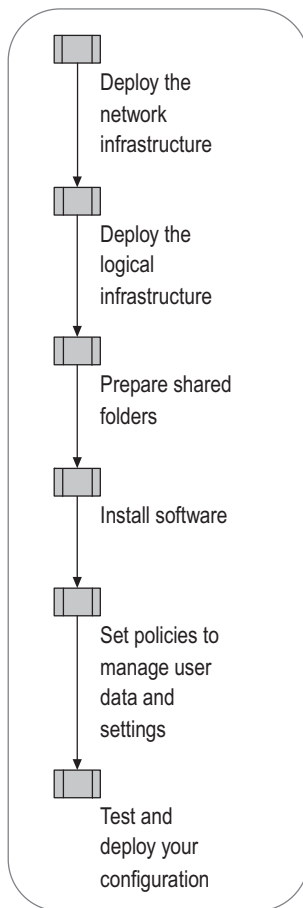
Create a small production environment If you are the system administrator of a small organization that wants to deploy a new network based on servers running the Microsoft® Windows® Server 2003 operating system, use the instructions here to build your initial production environment from the ground up, adding client computers and additional servers as needed. Be sure to follow all of the testing procedures included in “Testing and Deploying Your Configuration” later in this chapter, before inviting users to start their production work in the environment.

Create a test environment If you are part of a large organization’s IT management team, use the guidelines and procedures in this chapter to build a test network for testing various implementations of Active Directory® directory service and Group Policy in Windows Server 2003. After the structure is in place and your work has been tested, staged, and deployed to your production network, you can continue to use this small network for modeling and testing new Group Policies.

Process for Deploying a Simple Managed Environment

By performing the procedures in this chapter, you will deploy a domain controller (DC) within your intranet, create a logical infrastructure, assign and publish application software, and set up policies to manage your users and computers. You will use Microsoft Software Update Services (SUS) to review, approve, and test critical operating system updates before deploying them to your clients, so that you are secure in the knowledge that the clients are fully protected from the latest security risks. The steps for deploying a simple managed environment are illustrated in Figure 9.1.

Figure 9.1 Deploying a Simple Managed Network



Chapter Assumptions and Sample Configuration

A sample configuration has been devised to illustrate the various steps in creating a simple managed environment. This sample consists of a fictional organizational unit (OU) structure. You might want to go through each step using the sample data before implementing your own design; or, you might prefer to work through this guide, replacing the samples with your actual OUs and user accounts.

Organizational Units in the Sample Configuration

The chapter steps you through the creation of the OU structure and the users described in Table 9.1.

Table 9.1 Example of an OU Structure for a Simple Managed Environment

User Name	User Requirements	Security Group	Organizational Unit	Computer Type
Florian Voss	Domain Administrator; roaming profile; offline files; redirected folders	Administrators RUPUsers	IT	Mobile
Hung-Fu Ting Christie Moon	No roaming profile; offline files; redirected folders; needs access to the Microsoft® Office productivity suite only.		Bookkeeping	Desktop
Nicole Holliday Tzipi Butnaru	Roaming profiles; offline files; redirected folders; needs access to Microsoft Office only.	RUPUsers	Sales	Mobile

The following common characteristics and groupings are important to remember when applying policies (discussed in “Setting Policies to Manage User Data and Settings” later in this chapter):

- All users have redirected folders and offline files, and need access to Microsoft® Office applications.
- All users except the members of the Bookkeeping OU have roaming user profiles (RUP).
- The users in the IT and Sales OUs have mobile computing needs, but they almost always connect to the local area network (LAN) over a fast link.
- The users in the IT OU need access to the Windows Server 2003 Administrative Tools Pack.

This fictitious OU exists in a fictitious company named A. Datum Corporation with the domain name of `adatum.com`.

Hardware Configuration and Assumptions

Certain hardware and network assumptions are made in this chapter, which might not be true of your own environment. Read this chapter with the understanding that you need to reject assumptions if they do not apply to your organization.

The hardware configuration outlined here is intended to supply the basic needed components for a simple environment. The infrastructure includes one mobile client computer and one desktop client computer to demonstrate management techniques for these two common types of client computers. One server is deployed, which takes on several roles: Active Directory domain controller, Domain Name System (DNS) server, secure software distribution point using Distributed File System (DFS), and Software Update Services (SUS) distribution server. This computer also contains all of the application software, user state, and user data files for the organization.

Organizations frequently deploy a second server to host applications, SUS, and user data and settings. With this configuration, the DC can maintain the highest possible performance in its primary role. However, for a small organization, one server usually can fulfill all of these roles.

It is highly recommended that, if possible, you deploy a second DC to provide backup and redundancy. With two domain controllers, if one DC becomes unavailable, users still can log on and access their data using the second domain controller. By default, if no DC is available, only users with cached credentials can log on to the network.

Having a second DC already in place provides a much faster method of restoring service to users than having to create a new DC and populate its information from an external backup source. The second DC contains a complete and up-to-date replica of the entire Active Directory database; if the hard disk or data is corrupted on one DC, the second DC ensures that you will not have to rebuild your OU structure or repopulate your Active Directory database. The addition of a second DC should be a primary upgrade consideration for scaling your initial network and keeping it highly available.

If you choose to add a second DC to your network, consider the following:

- Replication affects network traffic. Place both DCs on the same network segment for best replication performance.
- A client computer can retrieve Group Policy objects (GPOs) from a DC to which a recent change has not yet been replicated.
- In a simple environment, it is recommended that you leave the operations master roles on one DC.



Note

For complete information about deploying multiple domain controllers in an Active Directory environment, see "Part 1: Designing and Deploying Directory Services" in *Designing and Deploying Directory and Security Services* of this kit.

Because this chapter's goal is to explain how to use change and configuration management techniques to manage a simple environment, the configuration that is presented does not include a second domain controller. The following assumptions and configuration are used in this chapter:

- Your network infrastructure does not include a secondary server or DC.
- The DC has one physical drive with two partitions. The first partition is logical drive C, and it will contain the Windows Server 2003 operating system. The second partition is logical drive D, and it will contain all software and user data that is not part of the operating system.
- The CD-ROM for the DC is logical drive E.

Minimum Hardware and Software Configurations for a Simple Managed Environment

To begin building your simple managed environment, use the minimum hardware and software configurations listed in Table 9.2. Your hardware list will expand to fit your organization's computing needs.

Table 9.2 Minimum Hardware and Software Configuration for a Simple Managed Environment

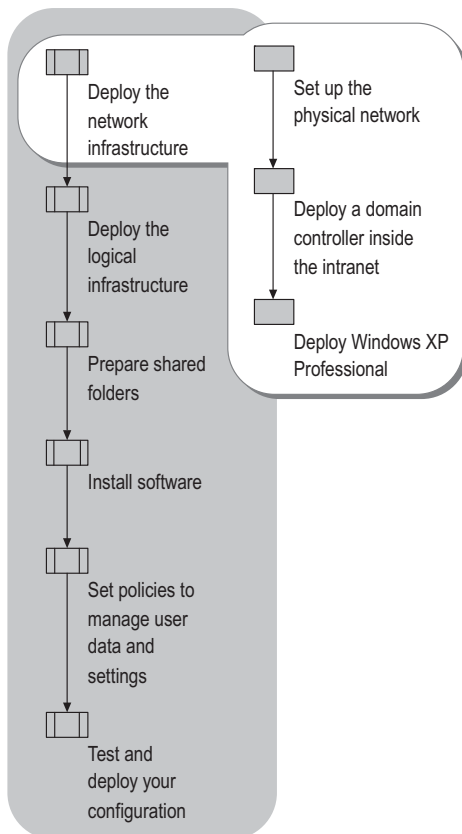
Device	Requirements
Domain controller running Windows Server 2003	See the Windows Server 2003 System Requirements link on the Web Resources page at http://www.microsoft.com/windows/reskits/webresources .
One desktop client computer running the Microsoft® Windows® XP Professional operating system	See the Windows XP Professional System Requirements link on the Web Resources page at http://www.microsoft.com/windows/reskits/webresources .
One mobile client computer running Windows XP Professional	See the Windows XP Professional System Requirements link on the Web Resources page at http://www.microsoft.com/windows/reskits/webresources .
Network Address Translator (NAT)-enabled router	Standard 5-port router recommended.
Broadband (cable or DSL) modem	No requirements.

Deploying the Network Infrastructure

Before implementing any management techniques, you must deploy your network infrastructure. In the chapter example, a Network Address Translation (NAT) router provides Dynamic Host Configuration Protocol (DHCP) addresses to all computers on the network, including the domain controller. Microsoft highly recommends the use of static IP addresses for domain controllers; however, in the sample configuration, the router does not continually release and renew leases, so the dynamic IP assigned to the domain controller is stable and essentially complies with that recommendation. If you want to assign a static IP address to your DC you can do so; however, this requires additional configuration that this chapter does not cover.

Figure 9.2 illustrates the steps involved in setting up the network infrastructure.

Figure 9.2 Deploying the Network Infrastructure



Setting Up the Physical Network

The components that you use in setting up your physical network will vary depending upon the equipment that you already have in place, your organization's specific needs, and the purpose of this network — that is, whether you are building a test LAN or an initial production LAN. The configuration documented here is that of a basic small network, which can be easily scaled to fit your computing needs. The router used here is a standard 5-port NAT router with a built-in firewall. Specific router instructions are not included, as those depend on the router that you have purchased.

► To configure your router

Follow the directions in the documentation for your router to configure the router to these specifications:

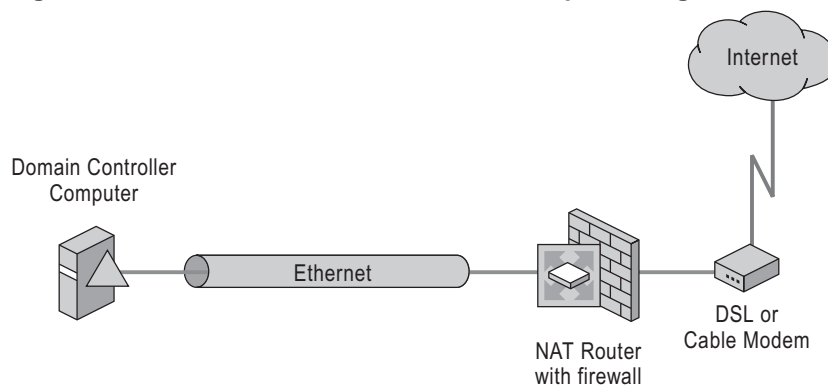
- Ensure that port 53 on the router is enabled to support DNS. (This is the default state of many routers.)
- If the router is wireless, enable 128-bit WEP security.
- Set a strong administrator password on the router.
- Use the instructions that you received with your router to configure the router to receive its IP configuration from your ISP using DHCP (this is the default state for many routers).

► To configure your LAN-router connection

1. Connect the LAN cable from the computer that is to be the DC to an available port on the NAT router.
2. Connect the LAN cable from the broadband modem to the WAN port on the NAT router.
3. Turn on the router and the modem.

Your network should be similar to the one illustrated in Figure 9.3.

Figure 9.3 LAN Router Connection for a Simple Managed Environment



Deploying a Domain Controller Inside the Intranet

You must deploy a domain controller (DC) in order to establish a top-level domain and forest on your private LAN.

For more information about domains and forests, see “Designing a Group Policy Infrastructure” in this book, and “Part 1: Designing and Deploying Directory and Security Services” in *Designing and Deploying Directory and Security Services* of this kit.

To deploy the DC, perform the following tasks:

- Install and configure the DC.
- Synchronize the timeserver for the domain controller with an external source.
- Format additional drive partitions.

Install and Configure the Domain Controller

To install and configure the domain controller, you will perform the following tasks:

- Install the Windows Server 2003 operating system.
- Install Active Directory on the domain controller, and configure the server role.
- Configure DNS.
- Install the Application Server role (Internet Information Services [IIS], ASP.NET). This step is only necessary for servers hosting Software Update Services (SUS) and is not a core requirement for a DC.

► **To install Windows Server 2003**

1. Boot from your Windows Server 2003 operating system CD-ROM. Follow the instructions in the documentation for Windows Server 2003 to install the operating system on the computer that is to be your domain controller. Create disk partitions with the following properties.

Partition	Use	File System	Size
Primary	Operating System	NTFS	At least 2 gigabytes (GB)
Secondary	Applications	NTFS	Remaining space



Note

If your LAN includes a second server, you can choose to create only one partition on the domain controller's hard drive, to store the operating system, and use the other server for storing additional software and data.

2. During Windows Setup, enter the following values:
 - **Computer Name:** Enter **DC01**.
 - **Administrator Password:** Enter a strong password.



Important

Computer security requires the use of a strong password for your administrator account. A strong password has from 7 through 14 characters, and contains letters (both uppercase and lowercase), numerals, and symbols (all other characters, such as \$%*&). The password should contain at least one symbol character in the second through sixth positions.

- **Network settings:** Select typical settings.
 - When prompted about whether this computer is part of a Workgroup or Computer Domain, select **Workgroup** and accept the default name of Workgroup.
3. After the computer restarts, log on as Administrator.
 4. Click **Start**, point to **All Programs**, and click **Activate Windows**. Follow the prompts to activate and register your copy of Windows Server 2003 through the Internet.

If you cannot access the Internet, refer to your router and modem instructions for troubleshooting assistance.

► **To configure the server as a domain controller**

1. Click **Start**, and click **Manage Your Server**. Select **Custom Configuration**. Click **Add or remove a role**, and then click **Next**. Wait for the wizard to review the computer's current configuration.
2. Select the **Domain Controller (Active Directory)** role. Proceed to run the Active Directory Installation Wizard. Use the following values as you are prompted for them:
 - a. Select **Domain controller for a new domain**.
 - b. Select **Domain in a new forest**.
 - c. Enter your domain name (in the sample configuration, this is **adatum.com**).
 - d. Accept the default values for **Domain NetBIOS name**, **Database folder**, **Log folder**, and **SYSVOL folder location**.

Because DNS has not yet been installed on this server, the **DNS Registration Diagnostics** will indicate that none of the DNS servers used by this computer responded within the timeout interval.

- e. Select **Install and configure the DNS server on this computer, and set this computer to use this DNS server as its preferred DNS server**.
- f. Select **Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems**.
- g. In the **Directory Services Restore Mode Administrator Password** field, enter a strong password.

The wizard will notify you that the computer has a dynamically assigned IP address. Typically you would not assign a dynamic IP address to a domain controller. However, this configuration is acceptable for this simple network in which the router is used as the DHCP server.

- h. When the **Local Area Connection Properties** page displays, click **Cancel**.
- i. When the wizard finishes configuring Active Directory, select **Restart Now**. After the computer has restarted, click **Finish**.

► **To configure the server as a DNS server**

1. From the **Manage Your Server** screen, click **Manage this DNS server**.
2. Right-click **DC01**, click **Configure a DNS Server**, and then click **Next**.
3. Select **Create a Forward Lookup Zone**.
4. Select **This server maintains the zone**. Type your domain name for the zone; for example, **adatum.com**.
5. Select **Allow dynamic updates**.
6. Select **Yes, forward queries to DNS servers with the following IP addresses**, and type the IP address of the NAT router.
7. Exit the **Manage DNS Server** snap-in.



Note

You will receive a message that the forward lookup zone cannot be added to the server, because the zone already exists. This is because the zone was created when the DNS server role was initially configured. This message does not indicate an error condition.

► **To install Application Server (IIS, ASP.NET)**

IIS is a necessary component for SUS. Use Manage Your Server to install IIS.

1. From the **Manage Your Server** screen, click **Add or remove a role**, and then click **Next**.
2. Select **Application Server (IIS, ASP.NET)**, and run the **IIS Installation** wizard. Do not load **FrontPage Server Extensions**, and do not **Enable ASP.NET** unless you need them for applications beyond the scope of this chapter.

► **To confirm that you have completed installing server roles**

1. In **Manage Your Server**, verify that your server has been configured with the following roles:
 - Application Server (for IIS)
 - Domain Controller (Active Directory)
 - DNS server
2. Close the **Manage your Server** program.

**Tip**

With Windows Server 2003, remote administration capability is built into the domain controller server role. Use the Remote Desktop for Administration program from any other computer to administer this server. As an extra security measure, it is recommended that you require smart card security for anyone who logs onto the DC remotely. For information about smart cards, see "Deploying Smart Cards" in *Designing and Deploying Directory and Security Services* of this kit. For more information about using Remote Desktop, see "Remote Desktop for Administration" in Help and Support Center for Windows Server 2003.

Synchronize the Time Server for the Domain Controller with an External Source

By default, the primary domain controller (PDC) emulator gets its time from the BIOS clock. In a network with a single DC, that DC automatically has this role. For more information about PDCs, see “Part 1: Designing and Deploying Directory Services” in *Designing and Deploying Directory and Security Services* of this kit.

The PDC emulator establishes the time and date settings for all computers within its domain. If the time is not accurately set in the PDC emulator’s BIOS, all computers in the domain have incorrect time and date settings.

To prevent this, you can synchronize the domain controller with an external time source such as the time servers provided by the National Institute of Standards and Technology (NIST). For a list of the names and IP addresses of NIST time servers for your area, see the National Institute of Standards and Technology (NIST) Internet Time Servers link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.



Note

Be aware that the Network Time Protocol (NTP) is unauthenticated, and unencrypted, and it is possible for an intruder to spoof the time root source, causing the wrong time to be set on the DC. You can avoid this possibility by using IPSec to secure the transmission, by accessing the time root source by its IP address rather than its fully qualified domain name, or by purchasing an NTP-capable hardware clock for your DC time synchronization.

► **To synchronize the domain controller with an external time source**

1. Click **Start**, and then click **Command Prompt**.
2. In the **Command Prompt** window, type the following line, where *peers* is a comma-separated list of IP addresses of the appropriate time sources, and press ENTER:
w32tm /config /manualpeerlist: *peers* /syncfromflags:MANUAL
 The time sources you choose depend on your time zone. For example, if your domain controller is located in the Pacific Time zone, this line might read:
w32tm /config /manualpeerlist:131.107.1.10 /syncfromflags:MANUAL
 In this example, the IP address of the timeserver is used instead of the fully qualified domain name for security purposes.
3. Press ENTER. You should get a message that the command completed successfully.
4. Type **w32tm /config /update**
5. Press ENTER. You should get a message that the command completed successfully.
 W32time uses a variable poll interval based on the quality of timesync with the server. On DCs, this interval defaults to between 64 and 1024 seconds.
6. To immediately synchronize with the external time server, type **w32tm /resync** and press ENTER. You should get a message that the command completed successfully.
7. Type **Exit** and press ENTER.

Format Additional Drive Partitions

You must format additional drive partitions on the domain controller before you can use them to store software and user data.

► **To format drive partitions**

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **Computer Management**.
2. Expand **Storage**, and click **Disk Management**.
3. In the right pane, right-click the volume (**D:**), and click **Format**.
4. Type a volume label that reflects the contents of this partition (such as **Apps**). Accept the other formatting defaults (**NTFS**, **default allocation unit size**), and click **OK**.
5. When formatting is complete, close the **Computer Management** snap-in.

Deploying Windows XP Professional

For the simple managed environment described in this chapter, client computer operating systems are installed manually. Alternatively, you can automate these installations as well as configure and deploy desktop images to specified computers throughout your domain. For more information about those capabilities, see “Designing Unattended Installations” in *Automating and Customizing Installations* of this kit.

The process of deploying Windows XP Professional includes these tasks:

- Deploying the client computers and installing the operating system
- Establishing the client’s IP addressing information
- Joining the client computer to the adatum.com domain
- Activating Windows and installing updates



Note

If the computer on which you are installing Windows XP has small computer system interface (SCSI) drives, and you receive the error message that “Setup did not find any hard disk drives installed in your system,” see article Q234054, “Error Message: Setup Did Not Find Any Hard Disk Drives Installed in Your System,” in the Microsoft Knowledge Base. To find this article, see the Microsoft Knowledge Base link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

► To deploy the client computers and install the operating system

1. Connect the client computers’ Ethernet connections to available ports on the router.
2. Follow the instructions in the documentation for Windows XP Professional to install the operating system on each client computer. Enter a strong password for the Administrator account. Use the default values for most settings, entering the following values when prompted.

Setting	Value	
	Desktop Computer	Laptop Computer
File System	NTFS	NTFS
User Name	Christie Moon	Tzipi Butnaru
Org Name	A. Datum Corporation	A. Datum Corporation
Computer Name	Desktop01	Laptop01
Network Settings	Typical	Typical
Domain/workgroup	Workgroup	Workgroup

► To establish the client's IP addressing information

It is important for the client's network configuration to contain the proper addressing information. To determine its addressing, perform the following steps.

1. Click **Start**, and click **Command Prompt**.
2. Type **ipconfig /all**, and press ENTER.
3. Make a note of the IP address, the default gateway, and the first listed DNS server.
The default gateway IP address must match the IP address of the NAT router. The first DNS server IP address must match that of DC01. If either address does not match the appropriate device, follow steps 4 through 7 to manually set the proper addresses.
4. Click **Start**, point to **Control Panel**, click **Network and Internet Connections**, and then click **Network Connections**.
5. Double-click **Local Area Connection**. Click **Properties**, select **Internet Protocol (TCP/IP)**, and click **Properties**.
6. Select **Use the following DNS server addresses**, and type the IP address of DC01 into this field.
7. Click **Advanced**. Under **Default gateways**, click **Add** and enter the IP address of your NAT router. Click **OK**, and close all windows.



Tip

Before joining the computer to the domain, use the TCP/IP **ping** command at the command prompt to test the connection to the IP addresses of DC01 and the NAT router in order to ensure that you can communicate to both devices.

► To join the client computer to the adatum.com domain

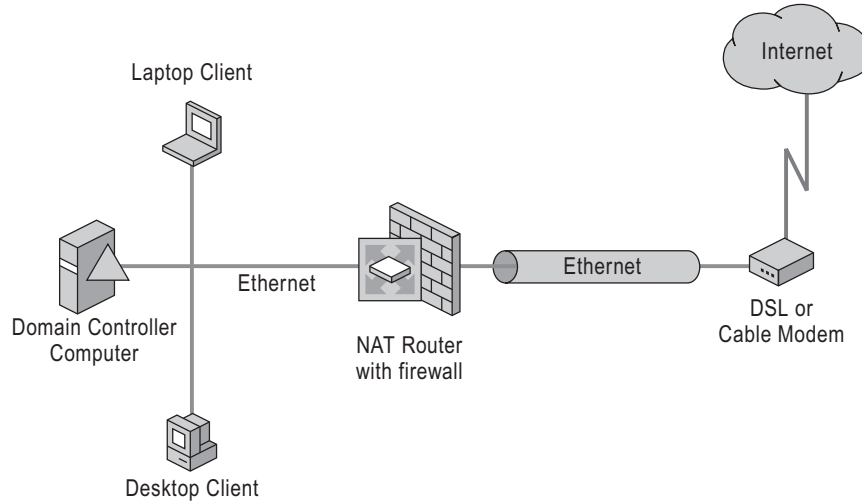
1. Click **Start**, click **My Computer**, and in the left pane, click **View system information**.
2. Click **Computer Name**, and click **Change**.
3. Click **Domain**, and type **adatum.com** as the domain name. When prompted for the name and password of a user who is authorized to join this computer to the domain, type **Administrator** and enter the strong password that you supplied for DC01.
4. You will receive a **Welcome to the adatum.com domain** message. Close all windows and reboot the client computer.

► **To activate Windows and install updates**

1. Log on to the client computer as its local Administrator.
2. Click **Start**, point to **All Programs**, and click **Activate Windows**. Follow the prompts to activate and register your copy of Windows XP Professional through the Internet.
3. Click **Start**, point to **All Programs**, and click **Windows Update**. Click **Pick updates to install**, then click **Review and install updates**.
4. Select and install **Windows XP SP1**. Follow the prompts to download and run the Windows XP Service Pack 1 Setup Wizard. Select the option **Do Not Archive Files**. After the service pack has been loaded, you are prompted to reboot. Do so and log on again as the local Administrator of this computer.
5. Click **Start**, point to **All Programs**, and click **Windows Update**. Click **Pick updates to install**. Remove all critical updates and service packs from the right pane (you will use Software Update Services to download approved critical updates to clients).
6. In the left pane, click **Windows XP**. In the right pane, click the **Add** button for **Microsoft .NET Framework**. Click **Review and install updates**. Follow the prompts to download and install **Microsoft .NET Framework**.

This completes the deployment of Windows XP to the client computers. The network infrastructure that you have created should be similar to the one in Figure 9.4.

Figure 9.4 Network Infrastructure with Clients Deployed



Deploying the Logical Infrastructure

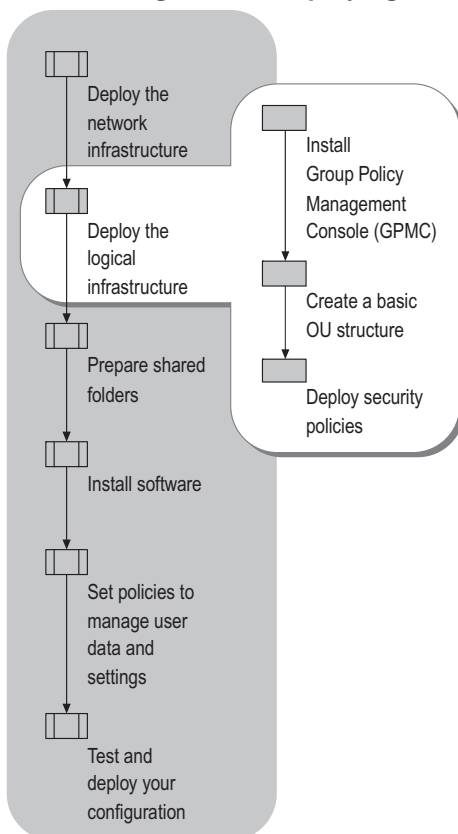
Before you can manage your environment, you must create an Active Directory structure. This structure includes organizational units (OUs) for users and computers, as well as security groups for assigning file share permissions. Use Group Policy Management Console (GPMC) and the Active Directory Computers and Users snap-in to develop this structure. Figure 9.5 shows the process for deploying the logical infrastructure for your simple managed environment.



Important

For all subsequent steps, you must log on to the domain controller with a domain administrator account unless otherwise instructed.

Figure 9.5 Deploying the Logical Infrastructure



Installing Group Policy Management Console (GPMC)

Group Policy Management Console (GPMC) unifies management of all aspects of Group Policy. Using GPMC, you can manage all Group Policy objects (GPOs), Windows Management Instrumentation (WMI) filters, and permissions on your network.

GPMC is available for download from the Microsoft Web site. For instructions for downloading and installing GPMC, see the Group Policy Management Console link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.



Tip

To access the GPMC download site, add Microsoft.com to your trusted sites in Microsoft® Internet Explorer.

► To run GPMC

- To open the GPMC snap-in, click **Start**, point to **Administrative Tools**, and click **Group Policy Management**.

Creating a Basic OU Structure

You need to create OUs for the users and computers you want to manage within your domain. This chapter uses a simple OU structure for a simple environment. If your environment requires a more complex OU structure, refer to the following documentation for planning information:

- “Designing a Group Policy Infrastructure” in this book.
- “Designing the Active Directory Logical Structure” in *Designing and Deploying Directory and Security Services* of this kit.

► **To create the OU structure**

1. Using GPMC, expand the forest node, the domains node, and the domain **adatum.com**.
2. Right-click **adatum.com**, and click **Active Directory Users and Computers**.
3. In the **Active Directory Users and Computers** MMC, expand **adatum.com**.
4. Right-click **adatum.com**, point to **New**, and click **Organizational Unit**.
5. For the new OU name, type **IT**.
6. Repeat steps 4 and 5 to create OUs named Bookkeeping and Sales.
7. Right-click the OU named IT, point to **New**, and click **User**.
8. Type the user information for Florian Voss, as shown in Table 9.1. Set the **User logon name** as Florian, and click **Next**.
9. When prompted for a **User Password**, type in a strong password. Make sure that **User must change password at next logon** is not checked.
10. Repeat steps 7 through 9 to create the user accounts within the appropriate OUs, as shown in Table 9.1.
11. With **adatum.com** highlighted, click **Builtin** in the left pane, and double-click **Administrators**.
12. Click **Members**, and click **Add**. In the **object names** text box, type **Florian**, and click **Check Names** to resolve the entry to Florian Voss. Click **OK**.
13. In the right pane, double-click **Domain Admins**.
14. Click **Members** and repeat step 12 to add Florian to the **Domain Admins** security group. Click **OK** twice, and click **adatum.com** in the left pane.
15. Right-click **adatum.com**, point to **New**, and click **Group**.
16. Type the group name **RUPUsers**. Make sure that the group type is **Security**, and that the group scope is **Global**.
17. Double-click the security group **RUPUsers**.
18. Click the **Members** tab, and click **Add**.
19. Click **Advanced**, and click **Locations**.
20. Expand **adatum**, click **Sales**, and click **OK**.
21. To select all users in the Sales OU, click **Find Now**. To add the users to the RUPUsers security group, click **OK**.
22. Repeat steps 17 through 19 to add all of the IT OU members to the RUPUsers security group.
23. Close the **Active Directory Users and Computers** snap-in, and minimize GPMC.

Although not addressed in this chapter's procedures, it is useful to understand that new user and computer accounts are created in the CN=Users and CN=Computers containers by default. It is not possible to apply Group Policy directly to these containers, although they inherit GPOs linked to the domain. Redirusr.exe (for user accounts) and Redircomp.exe (for computer accounts) are two new tools included with Windows Server 2003 that enable you to change the default location where new user and computer accounts are created so you can more easily scope GPOs directly to newly created user and computer objects. These tools are located in %windir%\system32.

By running Redirusr.exe and Redircomp.exe once for each domain, the domain administrator can specify the OUs into which all new user and computer accounts are placed at the time of creation. This allows administrators to manage these unassigned accounts by using Group Policy before the administrators assign them to the OU in which they are finally placed. You might want to consider restricting the OUs used for new user and computer accounts using Group Policy to increase security around new accounts.

For more information about redirecting users and computers, see article 324949, "Redirecting the Users and Computers Containers in Windows Server 2003 Domains," in the Microsoft Knowledge Base. To find this article, see the Microsoft Knowledge Base link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

For information on Redirusr.exe and Redircomp.exe, see the Redirecting Users and Computers link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

For additional information about these tools, see "Designing a Group Policy Infrastructure" in this book.

Deploying Security Policies

It is beyond the scope of this chapter to prescribe the security measures that you should take to protect your computing environment. Some things to consider are:

- Protect your physical equipment. For example, you might want to keep your domain controller computer inside a locked room or cabinet.
- Secure data as it traverses the network. If you are using Encrypting File System (EFS) to encrypt files, keep in mind that encrypted data is not encrypted when in transit over the network, but only when stored on disk. EFS does not work with roaming user profiles; if users encrypt files that are stored in their roaming profile, they will receive an error message when the profile is saved to the server. (You can, however, use IPSec in combination with EFS to protect the data when it is in transit.)

For more information about securing data as it traverses a network, see “Deploying Security Policy” in this book and “Deploying IPSec” in *Deploying Network Services* of this kit.

- If you have a wireless network, be sure to enable 128-bit WEP protection. Consider deploying Group Policy settings specifically designed to protect your data in a wireless environment; for more information, see “Deploying Security Policy” in this book.

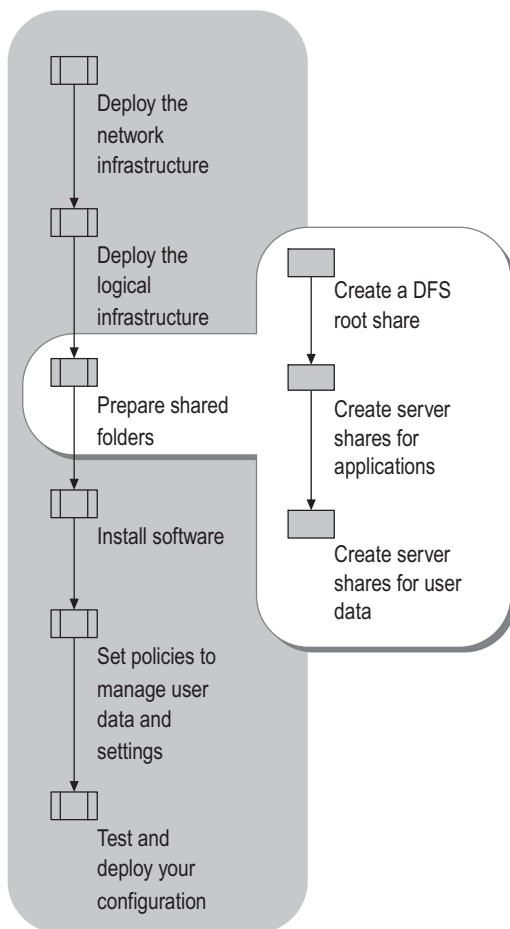
For more information about Group Policy and security policies, see “Designing a Group Policy Infrastructure” and “Deploying Security Policy” in this book. For best practices and considerations for securing user data and settings, see “Implementing User State Management” in this book. For more information about how to secure your Windows computing environment, see “Part 2: Deploying Distributed Security Services” in *Designing and Deploying Directory and Security Services* of this kit.

It is recommended that you deploy your selected security measures before continuing with the tasks in this chapter. If you are not ready to do so, you can proceed with the tasks, but be sure to secure your system before you deploy in a production environment.

Preparing Shared Folders

The next step in deploying your managed environment is to create a DFS root share to provide virtual views of the file shares. DFS is deployed to create scalable and flexible software distribution points. Next, you will prepare shared folders that will contain application software and user data (roaming user profiles and redirected folders). These steps are illustrated in Figure 9.6.

Figure 9.6 Preparing Shared Folders



Creating a DFS Root Share

Even though this chapter pertains to a very simple environment with only one server, setting up DFS when you initially install and deploy your applications can save you a lot of time later on when your organization grows. You can add additional and distributed storage capacity to the DFS namespace without changing the way your users access the data.

When creating a DFS namespace, you create either a stand-alone DFS root or a domain-based DFS root. Stand-alone DFS is an appropriate choice in cases where:

- Your organization does not use Active Directory.
- You need to create a DFS namespace and you are not part of the Domain Admins group, or company policy prevents you from delegating authority to manage a domain-based DFS namespace.
- You need to create a single namespace with more than 5,000 links. (If you can divide your links among two or more namespaces, domain-based DFS is an option.)
- You want to ensure the availability of the namespace by clustering the Distributed File System.

The chapter example sets up the DFS shares as domain-based because:

- The anticipated number of links is less than 5,000 links.
- No clustering hardware is deployed.
- Administration of DFS is centralized.
- The organization is using Active Directory, with the anticipation of using File Replication service (FRS) for replication once additional servers are added to the configuration.

For more information about DFS and FRS, see “Designing and Deploying File Servers” in *Planning Server Deployments* of this kit.

► **To set up DFS**

1. In Windows Explorer, navigate to **D:**.
2. On the **File** menu, click **New**, click **Folder**, type **UserApps**, and press ENTER.
3. Right-click the **UserApps** folder, and then click **Sharing and Security**.
4. Select **Share this folder**, and then accept the default share name of **UserApps**.
5. Click **Permissions**, and with **Everyone** highlighted in the top pane, click **Remove**.
6. Click **Add**, and then type: **auth**. Click **Check Names**, and your field entry resolves to the **Authenticated Users** built-in security group with the default permission of **Read**. Click **OK**.
7. Click **Offline Settings**.
8. Select **Files or programs from the share will not be available offline**, and then click **OK**.
9. Minimize Windows Explorer.
10. On the **Start** menu, point to **Programs**, point to **Administrative Tools**, and then click **Distributed File System**.
11. In the left pane, right-click **Distributed File System**, and then click **New Root**.
12. In the **New root wizard**, click **Next**, select **Domain root**, and then accept **adatum.com** as the domain to host the root.
13. In the **server name** field, type **DC01**.
14. In the **Root name** field, type **Public**, and click **Next**.
15. In the **Folder to share** field, type **D:\Public**, and then click **Yes** to create the folder.
16. Click **Finish** to complete the wizard.
17. In the left pane, right-click **\\adatum.com\Public**.
18. Click **New Link**, and for the link name, type **UserApps**. In **Path to target**, type **\\dc01\UserApps**.
This path can now be accessed as **\\adatum.com\Public\UserApps**.
19. Close the **Distributed File System** snap-in.

Completion of these steps creates a DFS root and link for use as a software installation point. You can add folders and applications in **UserApps**, or you can add other links to other physical locations that contain software packages you want to deploy using Group Policy. Doing this insulates the system from future changes to the underlying file servers and shares.

Creating Server Shares for Applications

For the chapter example, two applications are installed: Microsoft Office and the Windows Server 2003 Administrative Tools Pack. Microsoft Office will be assigned to all computers in the organization; the Administrative Tools Pack will be published to the IT OU only. For more information about assigning and publishing software using Group Policy, see “Deploying a Managed Software Environment” in this book.



Important

Although it is not specifically covered in this chapter, it is highly recommended that you purchase and assign virus protection software to all computers in the domain.

► To prepare a server share for Microsoft Office

Create a folder for Microsoft Office in the UserApps share. It inherits the file permissions from the parent folder.

1. Maximize Windows Explorer.
2. Navigate to D:\\UserApps and on the **File menu**, click **New**, click **Folder**, and type **MSOffice**. Press ENTER.

► To prepare a server share for the Administrative Tools Pack

Create a folder for system administrator tools in the UserApps share. (These steps assume you are already in Windows Explorer on DC01.)

1. In **D:\\UserApps**, on the **File menu**, click **New**, click **Folder**, and then type **AdminTools**. Press ENTER.
2. Right-click the **AdminTools** folder, and then click **Sharing and Security**.
3. Click the **Security** tab.
4. Click **Advanced**, and then uncheck **Allow inheritable permissions from the parent to propagate to the object and all child objects**.
5. Click **Remove** to confirm the action, and then click **OK**.
6. Only the **Administrators (ADATUM\\Administrators)** group is displayed in the top pane. Select this group, click **Full Control** in the bottom pane, and then click **OK**.

The preceding procedure allows full control for the **Administrators** group and allows no access for any other users.

Creating Server Shares for User Data

Some of the users in the chapter example OU have roaming user profiles, and all of them have redirected folders. You must create server shares on DC01 and apply the appropriate permissions.

- ▶ **To prepare a server share for roaming user profiles**
 1. On \\DC01, click **Start**, and then click **Windows Explorer**.
 2. Expand **My Computer**, and click drive **D:**.
 3. Click **File**, click **New**, click **Folder**, and type **RUP** into the **New Folder** text box. Press ENTER.
 4. Make the folder a network share. To set user permissions:
 - a. Right-click the **RUP** folder, and click **Sharing and Security**.
 - b. Select **Share this folder**. For the Share name, type **RUP\$**. (The \$ hides the share so that it is not visible in **My Network Places**.)
 - c. Click **Permissions**.
 - d. Click **Add**, and type **RUP** in the **Object Names** text box. Click **Check Names** to resolve the entry to the **RUPUsers** security group. Click **OK**.
 - e. With **RUPUsers** highlighted in the top pane, click **Allow** next to **Full Control** in the bottom pane. Click **OK**.
 - f. Click **Offline Settings**.
 - g. Select **Files or programs from the share will not be available offline**. (If you do not turn off Offline Folders for a user's profile, you can experience synchronization problems as both Offline Folders and Roaming Profiles try to synchronize the files in a user's profile.)
 - h. Click the **Security** tab. Click **Add** and type **RUP** in the **Object Names** text box. Click **Check Names** and it will resolve to the **RUPUsers** security group. Click **OK**.
 - i. With **RUPUsers** highlighted in the top pane, click **Allow** next to **Full Control** in the bottom pane. Click **OK**.

► **To prepare a server share for redirected folders**

Create a network file share on DC01 to contain all the individual user folders that will be redirected. These steps assume you are already in **Windows Explorer** and have drive D expanded.

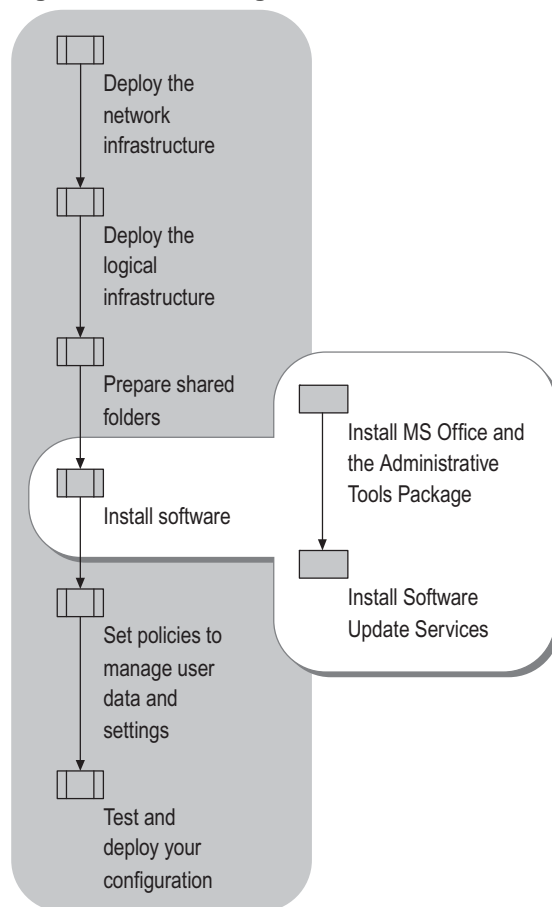
1. Click **File**, click **New**, click **Folder**, and type **Redir** into the **New Folder** text box. Press ENTER.
2. Make the folder a network share. To set user permissions:
 - a. Right-click the **Redir** folder, and click **Sharing and Security**.
 - b. Select **Share this folder**. Create the share name of **Redir\$**. Click **Permissions**, and with **Everyone** highlighted in the top pane, click **Remove** in the bottom pane.
 - c. Click **Add**, and type **auth** in the **Object Names** text box. Click **Check Names**, and the entry will resolve to the **Authenticated Users** built-in security group.
 - d. With **Authenticated Users** highlighted in the top pane, click **Allow** next to **Full Control** in the bottom pane. Click **OK**.
 - e. Click the **Security** tab. Click **Add**, and type **auth** in the **Object Names** text box. Click **Check Names**, and the entry will resolve to the built-in **Authenticated Users** security group. Click **OK**.
 - f. With **Authenticated Users** highlighted in the top pane, click **Allow** next to **Full Control** in the bottom pane.
 - g. With **Everyone** highlighted in the top pane, click **Remove** in the bottom pane. Click **OK**.

Following the preceding steps, you have created server file shares for roaming user profiles and redirected folders. You have set the permissions appropriately for the users who will need access to the shares, while denying access to other users.

Installing Software

Two types of software are installed on the domain controller: application software for users and Software Update Services (SUS), an administrative software package for reviewing and distributing critical and security operating system updates. Figure 9.7 illustrates the steps you will perform to install this software.

Figure 9.7 Installing Software



Installing MS Office and the Administrative Tools Package

By performing the previous procedures, you created server shares and set up DFS software distribution points. You must now perform an administrative installation of the software so that it can properly load onto client computers.

- ▶ **To perform an administrative installation of Microsoft Office**
 1. On the domain controller, insert the installation CD for Microsoft Office. When the Microsoft Office splash screen displays, close it.
 2. Click **Start**, and then click **Command Prompt**.
 3. To perform an administrative installation of the software, type **E:\setup /a**.
 4. Enter the product key for your copy of Microsoft Office.
 5. When prompted for the location in which to install Microsoft Office, navigate to **d:\UserApps\MSOffice**.
 6. When the installation of MS Office is complete, insert the Windows Server 2003 operating system CD into the CD-ROM drive. When the splash screen is displayed, close it.

► **To install the Windows Server 2003 Administrative Tools Pack**

- At the command line, type the following entry, and press ENTER:

COPY E:\I386\ADMINPAK.MSI D:\USERAPPS\ADMINTOOLS

All software is ready to assign and publish using Group Policy (in “Setting Policies to Manage User Data and Settings” later in this chapter).



Note

Be sure that you purchase the appropriate number of licenses for the software that you install. In many cases, you need to purchase a multiuser version of an application software package in order to perform an administrative install. Check with your software vendor for more information.

Installing Software Update Services

Software Update Services (SUS) helps you collect, approve, and distribute critical operating system updates to resolve security vulnerabilities and stability issues. In this chapter, SUS is used to distribute such updates to the Windows XP-based clients in the domain. For more information about deploying SUS, see “Deploying Software Update Services” in this book, and see the Software Update Services Deployment White Paper link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Perform the following procedure to install SUS version 1.0 with Service Pack 1 (SP1) on DC01.



Note

To use SUS on a DC, you must install SUS version 1.0 with SP1 or later.

► **To install SUS 1.0 SP1**

1. To download the SUS 1.0 SP1 server component, click the Software Update Services Download Site link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>, and follow the instructions.
2. When prompted to specify whether to open or save the file, click **Open**.
SUS will be downloaded and installed into a folder named \SUS on the largest drive partition available on DC01.
3. Choose the **Typical** setup.
After the wizard installs SUS, it provides you with a URL for administering SUS on DC01 (at <http://DC01/SUSAdmin>) and opens that Web page in Internet Explorer.
4. In the left pane of the SUS Administration Page, click **Set Options**.
5. Select the **Synchronize directly from the Microsoft Windows Update servers** option.
6. Select **Automatically approve new versions of previously approved updates**.
7. Accept the default for saving updates to a local folder, and click **Clear All** to uncheck all languages. Then select only those languages that you need in your environment. For the chapter example, check **English**. When you finish selecting languages, click **Apply**.
8. To download updates from the Microsoft Windows Update Server, in the left pane, click **Synchronize server** and then click **Synchronize Now**.
9. After downloading the updates, sort them by **Platform**. Select all Windows XP updates, and click **Approve**.
10. Click **Synchronize server** again, and click **Synchronization Schedule**. Set SUS to synchronize updates with the Microsoft Windows Update servers at 23:00 on Sunday.
11. Close the SUS Administration Page window.

You will use SUS later to download critical updates to the client computers.



Caution

This configuration is appropriate when you are administering SUS locally; if you need to administer SUS remotely, you should enable secure Hypertext Transfer Protocol Secure/Secure Sockets Layer (HTTPS/SSL). Deploying this option is beyond the scope of this chapter, but it is fully documented in "Deploying Software Update Services" in this book.

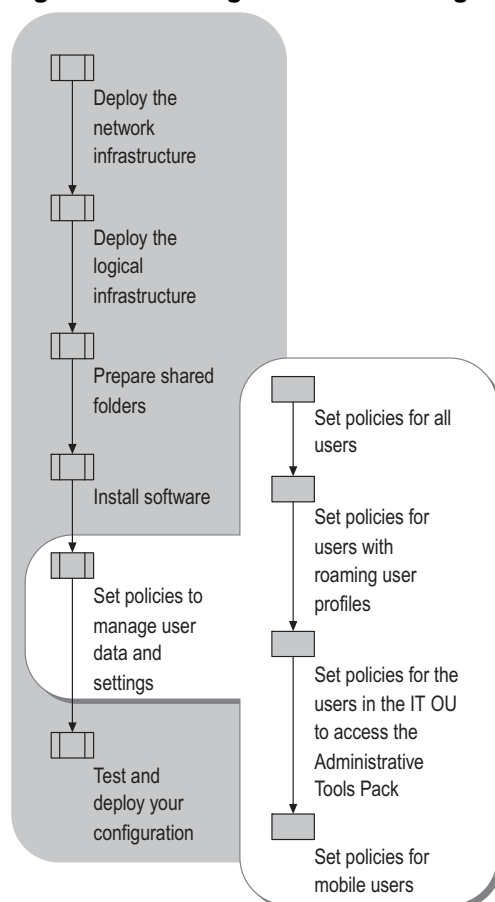
Setting Policies to Manage User Data and Settings

Group Policy settings determine how user state is managed in the environment described in this chapter. For information about managing user state with different types of users and different requirements, and for a fuller understanding of the range of options available for doing so, read “Implementing User State Management” in this book.

If you have questions about any specific GPO setting, you can click the **Explain** tab when that setting is being edited. The **Explain** tab provides a brief description of the setting and how to anticipate its applied result.

Figure 9.8 shows the steps involved in this part of your configuration.

Figure 9.8 Setting Policies to Manage User Data and Settings



Setting Policies for All Users

In the chapter example, all users have redirected folders and offline files, and they all need access to Microsoft Office applications. Windows Update on the client computers must be configured for SUS. As an administrator, you also want to limit the amount of shared disk space that any one user can absorb. Use the following sets of procedures while logged on to DC01 to set up this part of your managed environment.

► **To create a GPO for all users**

1. If GPMC is not already running on DC01, click **Start**, point to **Programs**, point to **Administrative Tools**, and click **Group Policy Management**.
2. In GPMC, expand **adatum.com**.
3. Expand **Group Policy Objects**. Right-click **Group Policy Objects**, and click **New**. When prompted for the **New GPO** name, type **All Users**, and click **OK**.

► **To set up folder redirection**

1. Right-click the **All Users** GPO, and click **Edit**.
2. Expand **User Configuration**, expand **Windows Settings**, click and expand **Folder Redirection**. Icons for the personal folders that can be redirected are displayed.
3. Right-click **My Documents** for redirection. (Note that when you redirect **My Documents**, all of its subfolders [**My Music**, **My Pictures**, and so forth] are automatically redirected as well; this is preferred.)
4. Click **Properties**, and in **Settings**, select **Basic - Redirect everyone's folders to the same location**.
5. Accept the default **Target folder location** of **Create a folder for each user under the root path**. Under the **Root Path** text box, type **\\dc01\redir\$**. Click **OK**.

This creates a unique folder for each user under **D:\Redir** on DC01.

► **To configure offline files**

1. Under **User Configuration** in the left pane, expand **Administrative Templates**, expand **Network**, and click **Offline Files**.
2. In the right pane, double-click **Do not automatically make redirected folders available offline**. Click **Disabled** and click **OK**. This setting ensures that redirected folders are always available when the user is offline.
3. In the right pane, double-click **Prohibit user configuration of Offline Files**. Click **Enabled**, and click **OK**.

This setting prevents users from disabling the offline file cache for My Documents, as well as preventing them from creating additional file caches. The use of this setting is discretionary.

4. In the right pane, double-click **Non-default server disconnect actions**. Click **Enabled**, and click **Show**.
5. In the **Show Contents** window, click **Add**, and type **DC01** as the name of the item to be added. Type **0** (zero) for the value, and click **OK** three times.

► **To configure Automatic Updates (Windows Update) for SUS**

1. Expand **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and click **Windows Update**.
2. In the right pane, double-click **Configure Automatic Updates**, and click **Enabled**.
3. Select the following options, and click **OK**:

- On the **Configure automatic updating** dropdown menu, select **4 - Automatically download and schedule the installation**. This choice is appropriate because no users are logging onto their computers as local administrators.
- On the **Scheduled install day** dropdown menu, select **every Monday**.
- On the **Scheduled install time** dropdown menu, select **21:00**. Click **OK**.

When this time and date arrive, updates will be downloaded and installed to the target computers.

4. In the right pane, double-click **Specify intranet Microsoft update service location**. Click **Enabled**, and in the **Set the intranet update service** text box, type **http://dc01/sus**. Type the same value in the **intranet statistics server** text box, and click **OK**.

► **To assign Microsoft Office to all authenticated users**

1. Under **User Configuration** in the left pane, expand **Software Settings**.
2. Right-click **Software Installation**, point to **New**, and click **Package**.
3. In the **File Open** dialog box, type `\\adatum.com\public\userapps\msoffice\`, click the appropriate .msi file, and click **Open**. (The name of the .msi file is dependent on the version of Office that you are installing.)

**Note**

It is important to use the UNC name of the share as described in step 3. If you navigate to the local location in lieu of entering the DFS Root share name and path, users will not be able to access the application.

1. Select **Assigned**, and click **OK**.
2. In the left pane, click **Software Installation**.

In the right pane, Microsoft Office is displayed as an assigned deployment.

**Note**

Make sure that you have the proper number of software licenses for the number of users who will use the application software.

► To set disk quotas

You can use disk quotas to manage disk space usage on the servers containing users' data. You can specify a disk quota limit and a disk quota warning level. For example, you can set a user's disk quota limit to 200 megabytes (MB), and the disk quota warning level to 150 MB. In this case, the user can store no more than 200 MB of files on the volume. If the user stores more than 150 MB of files on the volume, a system event is logged.

For more information about disk quotas, see "Implementing User State Management" in this book.

1. Expand **Computer Configuration**, expand **Administrative Templates**, and expand **System**. Click **Disk Quotas**.
2. In the right pane, double-click **Enable disk quotas**. Click **Enabled**, and click **OK**.
3. In the right pane, double-click **Enforce disk quota limit**. Click **Enabled** and click **OK**.
4. In the right pane, double-click **Default quota limit and warning level**. Click **Enabled**. Set the default quota limit to 200 MB. Scroll down and set the **Default warning level** to 150 MB, and click **OK**.
5. In the right pane, double-click **Log event when quota limit exceeded**. Click **Enabled**, and click **OK**.
6. In the right pane, double-click **Log event when quota warning level exceeded**. Click **Enabled**, and click **OK**.
7. In the right pane, double-click **Apply policy to removable media**. Click **Disabled**, and click **OK**.
8. Close the GPO editor.
9. If you want to view the settings that you just applied to this GPO, in GPMC, click the **All Users** GPO, click **Settings**, then click **show all**.



WARNING

Be careful when setting disk quotas for users who have roaming profiles. If you set those users' disk quotas too low, they can run out of profile space and be unable to log off. The 200 MB storage limit is an estimate of the amount of storage that the typical user needs. You should analyze your own user data patterns before setting this limit in your production environment.

Setting Policies for Users with Roaming User Profiles

In the chapter example, all users except for the members of the Bookkeeping OU have roaming user profiles. The GPO that you create here will be linked to those users in a subsequent procedure.

► **To create roaming user profile paths**

1. In GPMC, right-click **adatum.com**, and click **Active Directory Users and Computers**.
2. Expand **adatum.com**, and double-click **RUPUsers** in the right pane.
3. Click the **Members** tab, double-click **Florian Voss**, and click the **Profile** tab.
4. In the **Profile path** text box, type `\\dc01\rup$\%username%` to create a directory called Florian in the RUP server share. Click **OK**.
5. Repeat steps 3 and 4 for the other users in the RUPUsers security group.
When each user logs on, the system will create a folder in the RUP share containing his or her roaming user profile. Each folder is identified by the user's logon name.
6. Close the **Active Directory Users and Computers** snap-in.

► **To create a better user experience with roaming user profiles**

1. In GPMC, right-click **Group Policy Objects**, and click **New**. When prompted for the **New GPO** name, type **Enhance RUP**, and click **OK**.
2. Right-click the **Enhance RUP** GPO and click **Edit**.
3. Expand **Computer Configuration**, expand **Administrative Templates**, expand **System**, and click **Logon**.
4. Double-click **Always wait for the network at computer startup and logon** in the right pane.

This GPO setting improves logon time for users with roaming user profiles.

5. Click **Enabled**, and click **OK**.

You cannot encrypt files that are part of a roaming user profile, so a Group Policy setting is used to disable EFS for RUP users. For more information about EFS and other security options, see “Deploying Security Policies” in this chapter.

6. Under **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, expand **Public Key Policies**, and right-click **Encrypting File System**.
7. Click **Properties**. Clear the check box for **Allow users to encrypt files using Encrypting File System (EFS)**. Click **OK**, and exit the Group Policy editor.
8. Close the GPO editor.



Note

This step disables EFS for all files on the computer, not just the files in the redirected My Documents folder. Because this example assumes that all user data is kept in My Documents, this setting in this case is appropriate. If your users save data to other areas on their disk and they want to encrypt those files using EFS, you should not enable this setting. If files within these users' roaming profiles are inadvertently encrypted with EFS, the user will receive an error message when the system tries to save their profile to the server.

Setting Policies for the Users in the IT OU to Access the Administrative Tools Pack

In a previous section, you created a server share with the appropriate permissions for the Windows Server 2003 Administrative Tools Pack. The final step to make this software available to administrative users is to publish it using Group Policy.

► To publish the Administrative Tools Pack

1. In GPMC, right-click **Group Policy Objects**, and click **New**. When prompted for the **New GPO** name, type **AdminTools**, and click **OK**.
2. Right-click the **Admintools** GPO, and click **Edit**.
3. Expand **User Configuration**, and expand **Software Settings**.
4. Right-click **Software Installation**, point to **New**, and click **Package**.
5. In the **File Open** dialog box, type `\\adatum.com\public\userapps\admintools\adminpak.msi`, and click **Open**.



Note

It is important to use the UNC name of the share as described in step 5. If you navigate to the local location in lieu of entering the DFS Root share name and path, users will not be able to access the application.

1. Select **Published**, and click **OK**.
2. To verify that the Administrative Tools Pack was published successfully, click **Software Installation** in the left pane.
The Administrative Tools package displays in the right pane as a published deployment.
3. Close the GPO editor.

Setting Policies for Mobile Users

Several users in the example organization are considered mobile users: they use laptop computers and access the LAN from a variety of locations.

For more information about user types and best practices, see “Implementing User State Management” in this book.

► To create a pleasant mobile user experience

These Group Policy settings help ensure that your mobile users have the best user experience when logging on to a managed environment.

1. In GPMC, right-click **Group Policy Objects**, and click **New**. When prompted for the **New GPO** name, type **Mobile Users**, and click **OK**.
2. Right-click the **Mobile Users** GPO, and click **Edit**.
3. Expand **Computer Configuration**, expand **Administrative Templates**, expand **System**, and click **User Profiles**.
4. In the right pane, double-click **Do not detect slow network connections**. Click **Disabled**, and click **OK**.
This GPO setting blocks the user from disabling slow-link detection.
5. In the right pane, double-click **Timeout for dialog boxes**. Click **Enabled**, and then click **OK** to accept the default value (30 seconds).
This GPO setting causes a message to display briefly, saying that the user is not receiving their RUP because the user is logged on over a slow link.
6. In the left pane, click **Scripts**. In the right pane, double-click **Maximum wait time for Group Policy scripts**. Click **Enabled**, and accept the default wait time of 600 seconds.
This setting prevents the user from having to wait for longer than the specified maximum wait time for a logon script to complete execution over a slow link.
7. Close the GPO Editor.

Testing and Deploying Your Configuration

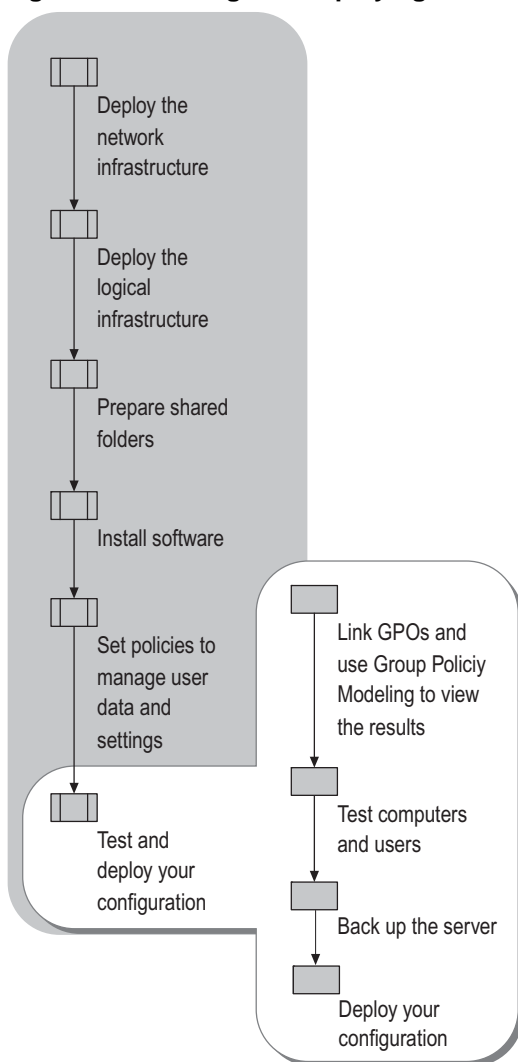
Most organizations have change management processes in place to ensure that any new configurations or deployments made to production systems go through rigorous testing within a non-production test environment prior to migration to production. This kind of change management process is especially important for Group Policy changes, because Group Policy can affect everything from registry settings to security settings to deployed software on a workstation or server. In addition to the many configuration settings that Group Policy accommodates, Group Policy objects can be linked to a number of different scopes, and their effect can be filtered by the use of user or computer security groups.

The ability to test Group Policy objects in a pre-production test environment, and to test the various ways that they can be deployed prior to committing them to live users and computers, is critical to maintaining your Windows infrastructure.

You should consider the testing phase to be essential to any successful Group Policy deployment. For complete information about testing and staging your group policies, see “Staging Group Policy Deployments” in this book.

Figure 9.9 illustrates the steps that you will take to test and deploy your configuration.

Figure 9.9 Testing and Deploying Your Configuration



Linking GPOs and Using Group Policy Modeling to View the Results

Now that you have created your GPOs, you can use GPMC to link them to your OUs and simulate the results.

► **To link a Group Policy object**

1. From within GPMC, expand and right-click the **Bookkeeping** OU.
2. Click **Link an Existing GPO**. Select the GPO named **All Users**, and click **OK**.

In the left pane, the **All Users** GPO is displayed beneath **Bookkeeping**.



Tip

You can simultaneously link multiple GPOs to an object by holding down the CTRL key while selecting GPOs.

► **To use Group Policy Modeling to simulate the application of GPOs**

1. To simulate the results, right-click **Group Policy Modeling**, and click **Group Policy Modeling Wizard**.
2. On the **User and Computer Selection** page, click the **User** option button, and click **Browse**.
3. Expand **adatum**, click **Bookkeeping**, and click **OK**. Click **Advanced**, and click **OK** to select all users in this group.
4. Select **Skip to the final page of this wizard without collecting additional data**, and click **Next**.

The **Summary of Selections** page displays the criteria that the wizard will use to process the simulation.

5. Click **Next**, and then click **Finish**.

The Group Policy modeling for **adatum.com/Bookkeeping** displays on the right side of the screen.

6. To view all settings, click **show all**.

As you scroll down the page, you will see that the All Users GPO has been applied to the Bookkeeping OU.

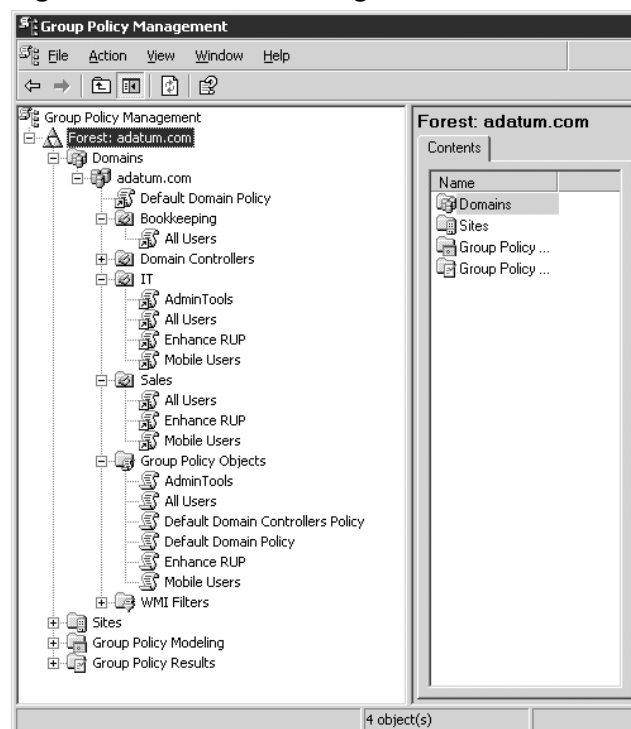
Continue to link GPOs as specified in Table 9.3.

Table 9.3 Group Policy Objects Linked to OUs

OU	Linked GPOs
Bookkeeping	All Users
IT	All Users, Enhance RUP, Mobile Users, Admin Tools
Sales	All Users, Enhance RUP, Mobile Users

7. When you have finished, the linked GPOs displayed in the left pane of GPMC should look like those in Figure 9.10.

Figure 9.10 GPMC Modeling Results



Testing Computers and Users

You must thoroughly evaluate your results before releasing this configuration to production users. Use this series of tests to validate your settings.

► To force an immediate update of linked GPOs, and review the results using Group Policy Results

By default, clients running Windows XP Professional, and servers running Windows Server 2003, check for changes to Group Policy objects every 90 minutes, plus or minus a random offset. Domain controllers running Windows Server 2003 check for computer policy changes every 5 minutes.

You can manually trigger a policy refresh by using the **gpupdate** command or by rebooting the client computers. The **gpupdate** command triggers a background policy refresh on the computer from which the command is run. For more information about the **gpupdate** command, see “Designing a Group Policy Infrastructure” in this book.

1. To force the linked GPOs to immediately take effect, reboot each client computer.
2. In GPMC on DC01, right-click **Group Policy Results**, and click **Group Policy Results Wizard**. On the **Computer Selection** page, click **Another computer** and type **Laptop01** into the name text box. On the User Selection page, click **ADATUM\Florian**. The Group Policy Results report in the right pane displays the combined settings for this computer and the selected user. You can save this report to disk or print it for your records.
3. Repeat step 2 to view the resultant set of policies for other computer and user combinations.

► To test computer and user configurations

Log on to each client computer as at least one user from each OU who would use that type of computer, as shown in Table 9.4 and Table 9.5. Perform the following steps.

1. Click **Start** and point to **All Programs**. The Office suite of programs should be listed.
2. Select Microsoft Excel, Microsoft Word, or other Office program. The software application will automatically install the first time the user accesses it. Thereafter, the program loads and runs when the user selects it.
3. When logged on as Florian, install the Administrative Tools Pack by using **Add or Remove Programs** in **Control Panel**. Those tools will then be available for Florian and other administrators from the **Start\Programs\Administrative Tools** menu.

The ability of users to install and run these applications is a confirmation that the assigned and published software programs are working correctly.

4. Check the Event Logs on each computer to make sure that no errors have occurred.

5. To test roaming user profiles, use one of the following methods:
 - Log on, log off, log on again, and then access the share \\dc01\RUP\$\%username%. The user's profile should have been copied to that share at logoff.
 - Make a simple change to a setting (for example, change the desktop background). Then log off and log on to another computer to make sure that the setting roams.
6. To test folder redirection, right-click **My Documents**, and click **Properties**. The **Target folder location** should point to the server share, not to the local computer.

If everything is installed and configured properly, users should have the settings and access to the applications listed in Table 9.4 and Table 9.5.

Table 9.4 Results for Users Logged On to Desktop01

Logon As	OU	Group Policy Settings	Applications
Hung-Fu	Bookkeeping	Offline Files Redirected Folders	Microsoft Office
Christie	Bookkeeping	Offline Files Redirected Folders	Microsoft Office

Table 9.5 Results for Users Logged On to Laptop01

Logon As	OU	Group Policy Settings	Applications
Nicole	Sales	Roaming User Profiles Offline Files Redirected Folders Mobile User Enhancements	Microsoft Office
Tzipi	Sales	Roaming User Profiles Offline Files Redirected Folders Mobile User Enhancements	Microsoft Office
Florian	IT	Roaming User Profiles Offline Files Redirected Folders Mobile User Enhancements	Microsoft Office Windows Server 2003 Administrative Tools Pack

Backing Up the Server

The importance of safeguarding your data by backing it up onto removable media cannot be overstated. Obtain a tape backup, writeable CD-ROM drive, or other suitable backup device for backing up your server and user data.

In the chapter example, user data is redirected to DC01, so backups of individual client machines are not necessary. Your own environment might require the ability to back up client hard drives as well as servers. After determining your backup needs, you can use the Backup program included in Windows Server 2003, or choose a third-party software program, to back up your data.

In addition to a backup device and software, you need a good backup plan. Many organizations perform a full server backup weekly, and then perform incremental backups (backing up only those files that have changed) each day.

Rotate your backup media. Using the backup scheme described in the preceding paragraph, you will need at least one set of backup media for each day of the week as well as a separate set of media for the fully weekly backups. Keep at least three separate sets on hand for rotation of the backups. In other words, use backup set 1 for one week; backup set 2 for the second week, and so forth.

Once a month, make a full system backup and data backup, and store the backup media offsite. In addition, make a system backup of your Active Directory database and the Sysvol folder on your DC — you will need this backup if you ever need to recover your Active Directory or Group Policy information. All of these backups should be considered permanent system archives, and not included in your rotation plan.

If you use tape cartridges for backup, re-tension the tapes after several uses. Replace tapes after six months of use. Tape erodes.

Always store your backup media offsite in a secure location — perhaps a safety deposit box or another office. In the event of disaster (flood or fire, for example), you want to be sure that you can recover all of your data.

In the chapter example, DC01 hosts Active Directory and all of its associated objects, as well as SUS, application software, RUPs, and redirected folders. Therefore, the information that must be backed up is stored in multiple locations on the computer. The subsequent procedures for backing up DC01 give you the basic commands for performing the various types of backup.

► To back up the entire contents of DC01

1. Click **Start**, point to **All Programs**, point to **Accessories**, point to **System Tools**, and click **Backup**.
2. Select **Backup Files and Settings**.
3. Select **All Information on this Computer**.
4. Designate where to save the data, click **Next**, and then click **Finish**.

► **To back up Active Directory and Group Policy**

1. Click **Start**, point to **All Programs**, point to **Accessories**, point to **System Tools**, and click **Backup**.
2. Select **Backup Files and Settings**.
3. Select **Let me choose what to back up**.
4. Navigate through drive C, and select the **System Volume** folder.
5. Scroll down, and click **System State**.
6. Designate where to save the data, click **Next**, and then click **Finish**.

These steps back up the current state of the domain controller (including Active directory settings and data) and Group Policy settings.

► **To back up GPOs**

It is very useful to make a backup of your GPOs, in the event that you need to restore only those settings, or want to copy them to another forest.

1. Click **Start**, and then click **GPMC**.
2. Expand **Forests**, expand **Domains**, and expand **adatum.com**.
3. Right-click **Group Policy Objects**, and click **Back Up All**.
4. Click **Browse**, and browse to the preferred storage location.

This might be a secure area on your server that will then be backed up onto tape, or you might back the Group Policy settings up directly on removable media.

5. Click **Backup**.

Note that you can also back up GPOs individually.

Another option for backing up GPOs in a domain is to use the BackupAllGPOs.wsf script, located in the %programfiles%\gpmc\scripts folder. The syntax for using the script requires that you provide the backup location and (optionally) a comment. For example, to back up GPOs in the adatum.com domain, you would enter the following command:

```
cscript BackupAllGPOs.wsf \\dc01\GPO-Backups /comment:"Weekly backup"
```

► **To back up data only**

1. Click **Start**, point to **All Programs**, point to **Accessories**, point to **System Tools**, and click **Backup**.
2. Select **Backup Files and Settings**.
3. Select **Let me choose what to back up**.
4. Navigate through drive C, and select **Redir**.

This folder contains all the redirected folders from the users. In the chapter example, all data is stored in these folders, so by backing up **Redir**, you are making a full data backup.

5. Designate where to save the data, click **Next**, and then click **Finish**.

Deploying Your Configuration

When you are completely satisfied with the results of your configuration, and have taken the time to back up the server, proceed to deploying the managed solution in your production environment. Be prepared to answer user questions regarding RUP and redirected folders. Explain disk quotas to users, so that they know what to do if they need additional shared storage space.

If the LAN that you created will be your new production environment, start migrating your users over to the LAN. If you have previous Windows-based clients and want to migrate existing user settings to the new environment, see “Migrating User State” in this book. You can scale this production network as your organization grows.

If this LAN will be a test environment, you can now back up your GPOs and restore them to your production environment. You can use the knowledge that you gained here to create new management solutions in that environment.

Deployment of a management solution is never a one-stop process. As your environment grows and changes, you will need to make adjustments in accommodation. The environment that this chapter develops is intended to give you the basic structure that will ease system management responsibilities as well as scale out to future demands.

Additional Resources

- “Part 1: Designing and Deploying Directory Services” in *Designing and Deploying Directory and Security Services* of this kit for information about designing and deploying your Active Directory infrastructure.
- “Deploying DNS” in *Deploying Network Services* of this kit for information about DNS.
- “Planning a Managed Environment” in this book for information about using IntelliMirror technologies to create a managed environment.
- “Deploying a Managed Software Environment” for information about using Group Policy to deploy application software to your users.
- “Designing a Group Policy Infrastructure” in this book for information about Group Policy.
- “Staging Group Policy Deployments” in this book for information about staging and testing your group policies.
- “Deploying Security Policy” in this book and “Part 2: Deploying Distributed Security Services” in *Designing and Deploying Directory and Security Services* of this kit for information about security.

- “Deploying IPsec” in *Deploying Network Services* of this kit for information about securing your data as it travels across the network.
- “Deploying Software Update Services” in this book, and the Software Update Services Deployment White Paper link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>, for information about SUS.
- “Overview of Deploying IIS 6.0” in *Deploying Internet Information Services (IIS) 6.0* of this kit for information about Internet Information Services (IIS).
- “Designing and Deploying File Servers” in *Planning Server Deployments* of this kit for information about file servers, DFS, and FRS.
- “Implementing User State Management” in this book for information about user profiles, folder redirection, disc quotas, and offline files.
- “Designing RIS Installations” in *Automating and Customizing Installations* of this kit for information about using RIS to deploy client operating systems and desktop images.

Glossary

Symbols

- .adm** The file name extension for Administrative Templates files.
- .msi** The file name extension for Windows Installer package files.

A

access control entry (ACE) An entry in an object's discretionary access control list (DACL) that grants permissions to a user or group. An ACE is also an entry in an object's system access control list (SACL) that specifies the security events to be audited for a user or group. See also access control list (ACL); discretionary access control list (DACL); object.

access control list (ACL) A list of security protections that apply to an entire object, a set of the object's properties, or an individual property of an object. There are two types of access control lists: discretionary and system. See also access control entry (ACE); discretionary access control list (DACL); object.

account lockout A Windows security feature that locks a user account if a number of failed logon attempts occur within a specified amount of time, based on security policy lockout settings. Locked accounts cannot log on.

ACE See definition for access control entry (ACE).

ACL See definition for access control list (ACL).

Active Directory The Windows-based directory service. Active Directory stores information about objects on a network and makes this information available to users and network administrators. Active Directory gives network users access to permitted resources anywhere on the network using a single logon process. It provides network administrators with an intuitive, hierarchical view of the network and a single point of administration for all network objects. See also domain; forest; object; replication.

Active Directory replication The synchronization of Active Directory partition replicas between domain controllers. Replication automatically copies the changes that originate on a writable directory partition replica to all other domain controllers that hold the same directory partition replica. More specifically, a destination domain controller pulls these changes from the source domain controller. See also Active Directory; domain controller; replica; replication.

Active Directory Service Interfaces (ADSI)

A directory service model and a set of Component Object Model (COM) interfaces. ADSI enables Windows applications and Active Directory clients to access several network directory services, including Active Directory. ADSI is supplied as a software development kit (SDK). See also Active Directory.

Active Directory Users and Computers

An administrative tool used by an administrator to perform day-to-day Active Directory administration tasks. The tasks that can be performed with this tool include creating, deleting, modifying, moving, and setting permissions on objects stored in the directory. Examples of objects in Active Directory are organizational units, users, contacts, groups, computers, printers, and shared file objects. See also Active Directory; object.

administrative credentials Logon information that is used to identify a member of an administrative group. Groups that use administrative credentials include Administrators, Domain Admins, and DNS Admins. Most system-wide or domain-wide tasks require administrative credentials. See also Administrators group.

administrative template (.adm file) A Unicode text file used by the Group Policy snap-in that defines which settings are displayed by the Group Policy user interface and indicates registry locations where changes are made. Windows NT 4.0 used an earlier version of .adm files for registry-based System Policy settings in the System Policy Editor. See also registry; Unicode.

administrator account On a local computer, the first account that is created when you install an operating system on a new workstation, stand-alone server, or member server. By default, this account has the highest level of administrative access to the local computer, and it is a member of the Administrators group.

In an Active Directory domain, the first account that is created when you set up a new domain by using the Active Directory Installation Wizard. By default, this account has the highest level of administrative access in a domain, and it is a member of the Administrators, Domain Admins, Domain Users, Enterprise Admins, Group Policy Creator Owners, and Schema Admins groups.

See also Active Directory; Administrators group; local computer; member server.

Administrators group On a local computer, a group whose members have the highest level of administrative access to the local computer. Examples of administrative tasks that can be performed by members of this group include installing programs; accessing all files on the computer; auditing access control; and creating, modifying, and deleting local user accounts.

In an Active Directory domain, a group whose members have the highest level of administrative access in the domain. Examples of administrative tasks that can be performed by members of this group include setting domain policy; assigning and resetting domain user account passwords; setting up and managing domain controllers; and creating, modifying, and deleting domain user accounts.

See also Active Directory; domain; domain controller; local computer; object.

application programming interface (API) A set of routines that an application uses to request and carry out lower-level services performed by a computer's operating system. These routines usually carry out maintenance tasks such as managing files and displaying information.

assigned application An application that is assigned to users or computers by an administrator using the Software Installation snap-in, which is an extension to Group Policy. Assigned applications are always available to users or computers managed by a Group Policy object. User-assigned applications appear to be installed on a user's computer and can be installed by selecting the software from the Start menu, or selecting a shortcut on the desktop. Applications assigned to a computer are installed when the computer is turned on.

assigning In Windows 2000, Windows XP, the Windows Server 2003 family, and Systems Management Server (SMS), to deploy a program to members of a group, where installation of the program is mandatory.

attribute For files, information that indicates whether a file is read-only, hidden, ready for archiving (backing up), compressed, or encrypted, and whether the file contents should be indexed for fast file searching.

In Active Directory, a property of an object. For each object class, the schema defines which attributes an instance of the class must have and which additional attributes it might have.

See also Active Directory; object; schema.

authentication The process for verifying that an entity or object is who or what it claims to be. Examples include confirming the source and integrity of information, such as verifying a digital signature or verifying the identity of a user or computer. See also Kerberos V5 authentication protocol.

authorization The process that determines what a user is permitted to do on a computer system or network. See also authentication.

B

bandwidth The data transfer capacity of a transmission medium.

In digital communications, the transfer capacity expressed in bits per second (bps) or megabits per second (Mbps). For example, Ethernet accommodates a bandwidth of 10,000,000 bps or 10 Mbps.

In analog communications, the difference between the highest and lowest frequencies in a specific range. For example, an analog telephone line accommodates a bandwidth of 3,000 hertz (Hz), the difference between the lowest (300 Hz) and highest (3,300 Hz) frequencies that it can carry.

See also bits per second (bps).

bits per second (bps) The number of bits transmitted every second, used as a measure of the speed at which a device, such as a modem, can transfer data.

C

cache A special memory subsystem in which frequently used data values are duplicated for quick access.

caching The process of temporarily storing recently accessed information in a special memory subsystem for quicker access. See also cache.

certificate A digital document that is commonly used for authentication and to secure information on open networks. A certificate securely binds a public key to the entity that holds the corresponding private key. Certificates are digitally signed by the issuing certification authority (CA), and they can be issued for a user, a computer, or a service.

child domain For DNS and Active Directory, a domain located in the namespace tree directly beneath another domain (the parent domain). For example, *example.microsoft.com* would be a child domain of the parent domain *microsoft.com*. Also known as a *subdomain*. See also Active Directory; domain; Domain Name System (DNS).

child object An object that resides in another object. A child object implies relation. For example, a file is a child object that resides in a folder, which is the parent object. See also object; parent object.

client Any computer or program connecting to, or requesting the services of, another computer or program. Client can also refer to the software that enables the computer or program to establish the connection.

For a local area network (LAN) or the Internet, a computer that uses shared network resources provided by another computer (called a *server*).

console A framework for hosting administrative tools, such as Microsoft Management Console (MMC). A console is defined by the items in its console tree, which might include folders or other containers, World Wide Web pages, and other administrative items. A console has windows that can provide views of the console tree and the administrative properties, services, and events that are acted on by the items in the console tree. See also console tree; Microsoft Management Console (MMC).

console tree The left pane in Microsoft Management Console (MMC) that displays the items contained in the console. The items in the console tree and their hierarchical organization determine the capabilities of a console. See also Microsoft Management Console (MMC).

cyclic redundancy check (CRC) A procedure used in checking for errors in data transmission. CRC error checking uses a complex calculation to generate a number based on the data transmitted. The sending device performs the calculation before transmission and sends its result to the receiving device. The receiving device repeats the same calculation after transmission. If both devices obtain the same result, it is assumed that the transmission was error-free. The procedure is known as a redundancy check because each transmission includes not only data but extra (redundant) error-checking values. Communications protocols such as XMODEM and Kermit use cyclical redundancy checking.

D

delegation An assignment of administrative responsibility to a user, computer, group, or organization.

For Active Directory, an assignment of responsibility that allows users without administrative credentials to complete specific administrative tasks or to manage specific directory objects. Responsibility is assigned through membership in a security group, the Delegation of Control Wizard, or Group Policy settings.

For DNS, an assignment of responsibility for a DNS zone. Delegation occurs when a name server (NS) resource record in a parent zone lists the DNS server that is authoritative for a child zone.

See also Active Directory; administrative credentials; Domain Name System (DNS); Group Policy; security group.

DFS root The starting point of the Distributed File System (DFS) namespace. The root is often used to refer to the namespace as a whole. A root maps to one or more root targets, each of which corresponds to a shared folder on a server. See also Distributed File System (DFS).

discretionary access control list (DACL) The part of an object's security descriptor that grants or denies specific users and groups permission to access the object. Only the owner of an object can change permissions granted or denied in a DACL; thus, access to the object is at the owner's discretion. See also access control entry (ACE); object; security group.

disk quota The maximum amount of disk space available to a user.

Distributed File System (DFS) A service that allows system administrators to organize distributed network shares into a logical namespace, enabling users to access files without specifying their physical location and providing load sharing across network shares.

distribution point A site system with the distribution point role that stores package files received from a site server. Clients contact distribution points to obtain programs and files after they detect that an advertisement is available from a client access point (CAP).

DNS See definition for Domain Name System (DNS).

domain In Active Directory, a collection of computer, user, and group objects defined by the administrator. These objects share a common directory database, security policies, and security relationships with other domains.

In DNS, any tree or subtree within the DNS namespace. Although the names for DNS domains often correspond to Active Directory domains, DNS domains should not be confused with Active Directory domains.

See also Active Directory; Domain Name System (DNS); object.

domain administrator A person who is a member of the Domain Admins group. Domain administrators can create, delete, and manage all objects that reside within the domain in which they are administrators. They can also assign and reset passwords and delegate administrative authority for network resources to other trusted users. See also domain; object.

domain controller In an Active Directory forest, a server that contains a writable copy of the Active Directory database, participates in Active Directory replication, and controls access to network resources. Administrators can manage user accounts, network access, shared resources, site topology, and other directory objects from any domain controller in the forest. See also Active Directory; authentication; forest.

domain DFS An implementation of Distributed File System (DFS) in which DFS topological information is stored in Active Directory. Because this information is made available on multiple domain controllers in the domain, domain DFS provides fault tolerance for any distributed file system in the domain. See also Active Directory; Distributed File System (DFS); fault tolerance.

domain hierarchy The parent/child tree structure of domains. See also domain.

domain migration The process of moving accounts, resources, and their associated security objects from one domain structure to another.

Domain Name System (DNS) A hierarchical, distributed database that contains mappings of DNS domain names to various types of data, such as IP addresses. DNS enables the location of computers and services by user-friendly names, and it also enables the discovery of other information stored in the database. See also IP address; ping; Transmission Control Protocol/Internet Protocol (TCP/IP).

Dynamic Host Configuration Protocol

(DHCP) A TCP/IP service protocol that offers dynamic leased configuration of host IP addresses and distributes other configuration parameters to eligible network clients. DHCP provides safe, reliable, and simple TCP/IP network configuration, prevents address conflicts, and helps conserve the use of client IP addresses on the network.

DHCP uses a client/server model where the DHCP server maintains centralized management of IP addresses that are used on the network. DHCP-supporting clients can then request and obtain lease of an IP address from a DHCP server as part of their network boot process.

See also IP address; Transmission Control Protocol/Internet Protocol (TCP/IP)

E

EFS See definition for Encrypting File System (EFS).

Encrypting File System (EFS) A feature in this version of Windows that enables users to encrypt files and folders on an NTFS volume disk to keep them safe from access by intruders. See also NTFS file system.

entry The lowest level element in the registry. Entries appear in the details pane of a Registry Editor window. Each entry consists of an entry name, its data type, and its value. Entries store the configuration data that affects the operating system and the programs that run on the system. As such, they are different from registry subtrees, keys, and subkeys, which are containers. See also key; registry.

Ethernet The IEEE 802.3 standard that uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) as the medium access control. Ethernet supports different mediums, such as coaxial cable, fiber-optic cable, and twisted-pair wiring, and different data rates, such as 10 megabits per second (Mbps).

F

fault tolerance The ability of computer hardware or software to ensure data integrity when hardware failures occur. Fault-tolerant features appear in many server operating systems and include mirrored volumes, RAID-5 volumes, and server clusters.

File Replication service (FRS) A service that provides multimaster file replication for designated directory trees between designated servers running Windows Server 2003. The designated directory trees must be on disk partitions formatted with the version of NTFS used with the Windows Server 2003 family. FRS is used by Distributed File System (DFS) to automatically synchronize content between assigned replicas and by Active Directory to automatically synchronize content of the system volume information across domain controllers. See also Active Directory; NTFS file system; replica; replication.

firewall A combination of hardware and software that provides a security system for the flow of network traffic, usually to prevent unauthorized access from outside to an internal network or intranet. Also called a *security-edge gateway*. See also proxy server.

Folder Redirection A Group Policy option that allows you to redirect designated folders to the network.

forest One or more Active Directory domains that share the same class and attribute definitions (schema), site and replication information (configuration), and forest-wide search capabilities (global catalog). Domains in the same forest are linked with two-way, transitive trust relationships. See also Active Directory; domain; schema.

forest functionality The functional level of an Active Directory forest that has one or more domain controllers running Windows Server 2003. The functional level of a forest can be raised to enable new Active Directory features that will apply to every domain in the forest. There are three forest functional levels: Windows 2000, Windows Server 2003 interim, and Windows Server 2003. The default forest functional level is Windows 2000. When the forest functional level is raised to Windows Server 2003 interim or Windows Server 2003, advanced forest-wide Active Directory features are available. See also Active Directory; domain; domain controller; forest.

forest root domain The first domain created in a new forest. The forest-wide administrative groups, Enterprise Admins and Schema Admins, are located in this domain. As a best practice, new domains are created as children of the forest root domain. See also child domain; domain; domain hierarchy; forest.

forward lookup A DNS query for a DNS name.
See also Domain Name System (DNS).

FRS See definition for File Replication service (FRS).

FSMO See definition for operations master.

G

global group A security or distribution group that can contain users, groups, and computers from its own domain as members. Global security groups can be granted rights and permissions for resources in any domain in the forest. See also member server.

globally unique identifier (GUID) A 16-byte value generated from the unique identifier on a device, the current date and time, and a sequence number. A GUID is used to identify a particular device or component.

GPMC See definition for Group Policy Management console (GPMC).

GPO See definition for Group Policy object (GPO).

Group Policy The infrastructure within Active Directory directory service that enables directory-based change and configuration management of user and computer settings, including security and user data. You use Group Policy to define configurations for groups of users and computers. With Group Policy, you can specify policy settings for registry-based policies, security, software installation, scripts, folder redirection, remote installation services, and Internet Explorer maintenance. The Group Policy settings that you create are contained in a Group Policy object (GPO). By associating a GPO with selected Active Directory system containers—sites, domains, and organizational units—you can apply the GPO's policy settings to the users and computers in those Active Directory containers. To create an individual GPO, use the Group Policy Object Editor. To manage Group Policy objects across an enterprise, you can use the Group Policy Management console. See also Active Directory; Group Policy Management console (GPMC); Group Policy object (GPO); Group Policy Object Editor.

Group Policy Management console (GPMC)

An optional tool that unifies and centralizes administration of Group Policy. See also Group Policy.

Group Policy Modeling A tool in Group Policy Management console that simulates what Group Policy settings are applied, given a specific set of criteria, including location of user or computer object in the directory, security group membership, and status of Windows Management Instrumentation (WMI) filters. You can use Group Policy Modeling to test new policy deployments before you deploy them. Also known as *Resultant Set of Policy—Planning Mode*. See also Group Policy Management console (GPMC); Group Policy Results; Resultant Set of Policy (RSOP); Windows Management Instrumentation filter.

Group Policy object (GPO) A collection of Group Policy settings. GPOs are essentially the documents created by the Group Policy Object Editor. GPOs are stored at the domain level, and they affect users and computers that are contained in sites, domains, and organizational units. In addition, each computer has exactly one group of policy settings stored locally, called the *local Group Policy object*. See also Group Policy; Group Policy Management console (GPMC); Group Policy Object Editor.

Group Policy Object Editor The Microsoft Management Console (MMC) snap-in that is used to edit Group Policy objects (GPOs). See also Group Policy Management console (GPMC); Group Policy object (GPO); Microsoft Management Console (MMC).

Group Policy Results A tool in Group Policy Management console that gathers information about which Group Policy settings have actually been applied to a specific computer, user, or both. You can use this tool to troubleshoot the application of Group Policy settings. Also known as *Resultant Set of Policy—Logging Mode*. See also Group Policy Management console (GPMC); Group Policy Modeling; Resultant Set of Policy (RSOP).

GUID See definition for globally unique identifier (GUID).

H

hash A fixed-size result that is obtained by applying a one-way mathematical function (sometimes called a *hash algorithm*) to an arbitrary amount of data. If there is a change in the input data, the hash changes. The hash can be used in many operations, including authentication and digital signing. Also called a *message digest*. See also authentication.

HTTP See definition for Hypertext Transfer Protocol (HTTP).

Hypertext Transfer Protocol (HTTP) The protocol used to transfer information on the World Wide Web. An HTTP address (one kind of Uniform Resource Locator (URL)) takes the following form: `http://www.microsoft.com`. See also Uniform Resource Locator (URL).

I-J

IIS See definition for Internet Information Services (IIS).

inheritance In security, a mechanism that allows a specific access control entry (ACE) to be copied from the container where it was applied to all children of the container. Inheritance can be used to manage access to a whole subtree of objects in a single update operation.

In Active Directory, the ability to build new object classes from existing object classes. The new object is defined as a subclass of the original object class. The original object class becomes a superclass of the new object. A subclass inherits the attributes of the superclass, including structure rules and content rules.

In Group Policy, a mechanism that allows policy settings in Group Policy objects (GPOs) that are linked to parent containers to be applied to objects in child containers.

See also access control entry (ACE); Active Directory; delegation; Group Policy Management console (GPMC); Group Policy object (GPO).

Integrated Services Digital Network (ISDN) A digital phone line used to provide higher bandwidth. ISDN in North America is typically available in two forms: Basic Rate Interface (BRI) consists of 2 B-channels at 64 kilobits per second (Kbps) and a D-channel at 16 Kbps; Primary Rate Interface (PRI) consists of 23 B-channels at 64 Kbps and a D-channel at 64 Kbps. An ISDN line must be installed by the phone company at both the calling site and the called site.

IntelliMirror A set of change and configuration management features based on Active Directory that enables management of user and computer data and settings, including security data. IntelliMirror also provides limited ability to deploy software to Windows 2000 and later workstations or servers. See also Active Directory.

Internet Information Services (IIS) Software services that support Web site creation, configuration, and management, along with other Internet functions. Internet Information Services include Network News Transfer Protocol (NNTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP).

Internet Protocol (IP) A routable protocol in the TCP/IP protocol suite that is responsible for IP addressing, routing, and the fragmentation and reassembly of IP packets. See also Transmission Control Protocol/Internet Protocol (TCP/IP).

Internet Protocol security (IPSec) A set of industry-standard, cryptography-based protection services and protocols. IPSec protects all protocols in the TCP/IP protocol suite except Address Resolution Protocol (ARP). For virtual private network (VPN) connections, IPSec is used in conjunction with Layer Two Tunneling Protocol (L2TP). See also Transmission Control Protocol/Internet Protocol (TCP/IP); virtual private network (VPN).

Internet Server Application Programming Interface (ISAPI) An application programming interface (API) that resides on a server computer for initiating software services tuned for Windows operating systems.

In Microsoft Provisioning System, ISAPI resides on the Web server.

See also application programming interface (API).

IP address For Internet Protocol version 4 (IPv4), a 32-bit address used to identify an interface on a node on an IPv4 internetwork. Each interface on the IP internetwork must be assigned a unique IPv4 address, which is made up of the network ID, plus a unique host ID. This address is typically represented with the decimal value of each octet separated by a period (for example, 192.168.7.27). You can configure the IP address statically or dynamically by using Dynamic Host Configuration Protocol (DHCP).

For Internet Protocol version 6 (IPv6), an identifier that is assigned at the IPv6 layer to an interface or set of interfaces and that can be used as the source or destination of IPv6 packets.

See also Dynamic Host Configuration Protocol (DHCP); Internet Protocol (IP); node.

IPSec See definition for Internet Protocol security (IPSec).

ISAPI See definition for Internet Server Application Programming Interface (ISAPI).

K

Kerberos V5 authentication protocol An authentication mechanism used to verify user or host identity. The Kerberos V5 authentication protocol is the default authentication service. Internet Protocol security (IPSec) can use the Kerberos protocol for authentication. See also Internet Protocol security (IPSec).

key In Registry Editor, a folder that appears in the left pane of the Registry Editor window. A key can contain subkeys and entries. For example, Environment is a key of HKEY_CURRENT_USER.

In IP security (IPSec), a value used in combination with an algorithm to encrypt or decrypt data. Key settings for IPSec are configurable to provide greater security.

See also entry; Internet Protocol security (IPSec); registry.

L

LAN See definition for local area network (LAN).

Lightweight Directory Access Protocol (LDAP) The primary access protocol for Active Directory. LDAP is an industry-standard protocol, established by the Internet Engineering Task Force (IETF), that allows users to query and update information in a directory service. Active Directory supports both LDAP version 2 and LDAP version 3. See also Active Directory.

load balancing A technique used by Windows Clustering to scale the performance of a server-based program (such as a Web server) by distributing its client requests across multiple servers within the cluster. Each host can specify the load percentage that it will handle, or the load can be equally distributed across all the hosts. If a host fails, Windows Clustering dynamically redistributes the load among the remaining hosts.

local area network (LAN) A communications network connecting a group of computers, printers, and other devices located within a relatively limited area (for example, a building). A LAN enables any connected device to interact with any other on the network. See also network basic input/output system (NetBIOS).

local computer The computer that you are currently logged on to as a user. More generally, a local computer is a computer that you can access directly without using a communications line or a communications device, such as a network adapter or a modem.

local user profile A computer-based record about an authorized user that is created automatically on the computer the first time a user logs on to a workstation or server computer.

M

mandatory user profile A user profile that is not updated when the user logs off. It is downloaded to the user's desktop each time the user logs on, and it is created by an administrator and assigned to one or more users to create consistent or job-specific user profiles. Only members of the Administrators group can change profiles. See also roaming user profile; user profile.

media access control (MAC) A sublayer of the IEEE 802 specifications that defines network access methods and framing.

member server A server that is joined to a domain but is not a domain controller. Member servers typically function as file servers, application servers, database servers, Web servers, certificate servers, firewalls, or remote access servers. See also domain; domain controller.

Microsoft Management Console (MMC)

A framework for hosting administrative tools called *snap-ins*. A console might contain tools, folders or other containers, World Wide Web pages, and other administrative items. These items are displayed in the left pane of the console, called a *console tree*. A console has one or more windows that can provide views of the console tree. The main MMC window provides commands and tools for authoring consoles. The authoring features of MMC and the console tree itself might be hidden when a console is in User Mode. See also console tree; snap-in.

MMC See definition for Microsoft Management Console (MMC).

N

namespace A naming convention that defines a set of unique names for resources in a network. For DNS, a hierarchical naming structure that identifies each network resource and its place in the hierarchy of the namespace. For WINS, a flat naming structure that identifies each network resource using a single, unique name. See also Domain Name System (DNS); Windows Internet Name Service (WINS).

NetBIOS See definition for network basic input/output system (NetBIOS).

network address translator (NAT) An IP router defined in RFC 1631 that can translate IP addresses and Transmission Control Protocol/User Datagram Protocol (TCP/UDP) port numbers as packets are forwarded. See also Internet Protocol (IP); IP address; Transmission Control Protocol/Internet Protocol (TCP/IP); User Datagram Protocol (UDP).

network basic input/output system (NetBIOS) An application programming interface (API) that can be used by programs on a local area network (LAN). NetBIOS provides programs with a uniform set of commands for requesting the lower-level services required to manage names, conduct sessions, and send datagrams between nodes on a network. See also application programming interface (API); local area network (LAN); node.

Network Connections A component you can use to gain access to network resources and functionality, whether you are physically at the network location or in a remote location. By using the Network Connections folder you can create, configure, store, and monitor connections. Formerly called *Network and Dial-up Connections* or *Dial-Up Networking*.

Network Load Balancing A component of Windows 2000 Server that provides high availability and scalability of servers by using a cluster of two or more host computers working together. Clients access the cluster using a single IP address.

Network Load Balancing cluster Up to 32 Web servers from which Network Load Balancing presents a single IP address to Web clients and among which Network Load Balancing distributes incoming Web requests. See also IP address.

node For tree structures, a location on the tree that can have links to one or more items below it.

For local area networks (LANs), a device that is connected to the network and is capable of communicating with other network devices.

For server clusters, a computer system that is an active or inactive member of a cluster.

See also local area network (LAN).

NTFS file system An advanced file system that provides performance, security, reliability, and advanced features that are not found in any version of file allocation table (FAT). For example, NTFS guarantees volume consistency by using standard transaction logging and recovery techniques. If a system fails, NTFS uses its log file and checkpoint information to restore the consistency of the file system. NTFS also provides advanced features, such as file and folder permissions, encryption, disk quotas, and compression.

O

object An entity, such as a file, folder, shared folder, printer, or Active Directory object, described by a distinct, named set of attributes. For example, the attributes of a File object include its name, location, and size; the attributes of an Active Directory User object might include the user's first name, last name, and e-mail address.

For OLE and ActiveX, an object can also be any piece of information that can be linked to, or embedded into, another object.

See also Active Directory; attribute; child object; parent object.

Offline Files An IntelliMirror management technology that allows network users to access files on network shares, even when the client computer is disconnected from the network. When a mobile user views the share while disconnected, the user can still work with the files because the files have been cached on the client computer. When the user later connects to the server, the system reconciles the changes with the server. See also IntelliMirror.

operations master A domain controller that has been assigned one or more special roles in an Active Directory domain. The domain controllers assigned these roles perform operations that are single-master (not permitted to occur at different places on the network at the same time). Examples of these operations include resource identifier allocation, schema modification, PDC emulation, adding and removing domains to and from the forest, and tracking changes to security principals across all domains in a forest. See also Active Directory; domain controller.

organizational unit An Active Directory container object used within domains. An organizational unit is a logical container into which users, groups, computers, and other organizational units are placed. It can contain objects only from its parent domain. An organizational unit is the smallest scope to which a Group Policy object (GPO) can be linked, or over which administrative authority can be delegated. See also Active Directory; Group Policy object (GPO).

ou See definition for: organizational unit

P-Q

parent object An object in which another object resides. For example, a folder is a parent object in which a file, or child object, resides. An object can be both a parent and a child object. For example, a subfolder that contains files is both the child of the parent folder and the parent folder of the files. See also child object; object.

ping A utility that verifies connections to one or more remote hosts. The **ping** command uses Internet Control Message Protocol (ICMP) echo request and echo reply packets to determine whether a particular Internet Protocol (IP) system on a network is functional. **Ping** is useful for diagnosing IP network or router failures. See also Internet Protocol (IP).

proxy server A firewall component that manages Internet traffic to and from a local area network (LAN) and that can provide other features, such as document caching and access control. A proxy server can improve performance by supplying frequently requested data, such as a popular Web page, and it can filter and discard requests that the owner does not consider appropriate, such as requests for unauthorized access to proprietary files. See also firewall; local area network (LAN).

public key infrastructure (PKI) The laws, policies, standards, and software that regulate or manipulate certificates and public and private keys. In practice, it is a system of digital certificates, certification authorities, and other registration authorities that verify and authenticate the validity of each party involved in an electronic transaction. Standards for PKI are still evolving, even though they are being widely implemented as a necessary element of electronic commerce. See also certificate.

published application An application that is available to users managed by a Group Policy object. Each user decides whether or not to install the published application by using **Add or Remove Programs** in Control Panel. See also Group Policy object (GPO).

QoS See definition for Quality of Service (QoS).

Quality of Service (QoS) A set of quality assurance standards and mechanisms for data transmission, implemented in this version of Windows.

R

registry A database repository for information about a computer's configuration. The registry contains information that Windows continually references during operation, such as: profiles for each user; the programs installed on the computer and the types of documents that each can create; property settings for folders and program icons; what hardware exists on the system; which ports are being used.

The registry is organized hierarchically as a tree, and it is made up of keys and their subkeys, hives, and entries.

See also entry; key.

remote access Part of the integrated Routing and Remote Access service that provides remote networking for telecommuters, mobile workers, and system administrators who monitor and manage servers at multiple branch offices. Users can use Network Connections to dial in to remotely access their networks for services such as file and printer sharing, electronic mail, scheduling, and SQL database access.

Remote Installation Server (RIS) An optional component that remotely installs Windows XP Professional. RIS installs the operating system on remote boot-enabled client computers by connecting the computer to the network, starting the client computer, logging on with a valid user account, and copying an operating system image to the client computer.

replica In Active Directory replication, one instance of a logical Active Directory partition that is synchronized by means of replication between domain controllers that hold copies of the same directory partition. *Replica* can also refer to an instance of an object or attribute in a distributed directory.

In the File Replication service (FRS), a computer that has been included in the configuration of a specific replica set.

See also Active Directory; File Replication service (FRS).

replication The process of copying updated data from a data store or file system on a source computer to a matching data store or file system on one or more destination computers to synchronize the data.

In Active Directory, replication synchronizes schema, configuration, application, and domain directory partitions between domain controllers.

In Distributed File System (DFS), replication synchronizes files and folders between DFS roots and root targets.

See also Active Directory; DFS root; Distributed File System (DFS); File Replication service (FRS); replica; topology.

resource domain A Windows NT 4.0 domain that is used for hosting file, print, and other application services. See also domain.

Resultant Set of Policy (RSOP) A feature that simplifies Group Policy implementation and troubleshooting. RSOP uses Windows Management Instrumentation (WMI) to determine how policy settings are applied to users and computers. RSOP has two modes: logging mode and planning mode. Logging mode determines the resultant effect of policy settings that have been applied to an existing user and computer based on a site, domain, and organizational unit. Planning mode simulates the resultant effect of policy settings that are applied to a user and computer. See also Group Policy; Group Policy Management console (GPMC); Microsoft Management Console (MMC); Windows Management Instrumentation (WMI).

RIS See definition for Remote Installation Server (RIS).

roaming profile A set of user-specific settings in a single location on a server so that users can move from computer to computer while retaining the same profile.

roaming user profile A server-based user profile that is downloaded to the local computer when a user logs on and that is updated both locally and on the server when the user logs off. A roaming user profile is available from the server when logging on to a workstation or server computer. When logging on, the user can use the local user profile if it is more current than the copy on the server. See also local user profile; mandatory user profile; user profile.

root The highest or uppermost level in a hierarchically organized set of information. The root is the point from which further subsets are branched in a logical sequence that moves from a broad or general focus to narrower perspectives. See also DFS root.

router A device or computer that forwards packets between interfaces based on a network layer destination address. For example, an Internet Protocol (IP) router forwards IP packets based on the destination IP address in the IP header. Routers typically use a routing table, which contains a series of entries for destinations and the corresponding next-hop address and interface to use to forward a packet to its eventual destination. See also local area network (LAN); wide area network (WAN).

S

schema The set of definitions for the universe of objects that can be stored in a directory. For each object class, the schema defines which attributes an instance of the class must have, which additional attributes it can have, and which other object classes can be its parent object class. See also attribute; object; parent object.

Secure Sockets Layer (SSL) A protocol that supplies secure data communication through data encryption and decryption. This protocol enables communications privacy over networks through a combination of public-key cryptography and bulk data encryption.

security filtering A method of applying the settings of a Group Policy object (GPO) based on security principals. See also Group Policy object (GPO).

security group A group that can be listed in discretionary access control lists (DACLS) used to define permissions on resources and objects. A security group can also be used as an e-mail entity. Sending an e-mail message to the group sends the message to all the members of the group. See also discretionary access control list (DACL).

security ID (SID) A data structure of variable length that identifies user, group, and computer accounts. Every account on a network is issued a unique SID when the account is first created. Internal processes in Windows refer to an account's SID rather than the account's user or group name.

security policies The account, user rights, and audit policies that are managed using User Manager. There are also trust relationship policies that apply to domain controllers.

security template A physical file representation of a security configuration that can be applied to a local computer or imported to a Group Policy object (GPO) in Active Directory. When you import a security template to a GPO, Group Policy processes the template and makes the corresponding changes to the members of that GPO, which can be users or computers. See also Active Directory; Group Policy; Group Policy object (GPO).

SID See definition for security ID (SID).

Simple Network Management Protocol (SNMP) A network protocol used to manage TCP/IP networks. In Windows, the SNMP service is used to provide status information about a host on a TCP/IP network. See also Transmission Control Protocol/Internet Protocol (TCP/IP).

site One or more well-connected (highly reliable and fast) TCP/IP subnets. A site allows administrators to configure Active Directory access and replication topology to take advantage of the physical network. See also Active Directory; Transmission Control Protocol/Internet Protocol (TCP/IP).

SMS See definition for Systems Management Server (SMS).

snap-in A type of tool that you can add to a console supported by Microsoft Management Console (MMC). A stand-alone snap-in can be added by itself; an extension snap-in can be added only to extend the function of another snap-in. See also Microsoft Management Console (MMC).

SNMP See definition for Simple Network Management Protocol (SNMP).

Software Update Services (SUS) A tool that is used to acquire and distribute critical Windows patches to computers running Windows 2000, Windows XP, and Windows Server 2003 operating systems. By using SUS, administrators can download the latest patches onto their intranet, test the patches in a standard operating environment, and then deploy the patches to the appropriate computers running the Automatic Updates client.

Synchronization Manager A tool used to ensure that a file or directory on a client computer contains the same data as a matching file or directory on a server.

synchronize To reconcile the differences between files stored on one computer and versions of the same files on another computer. Once the differences are determined, both sets of files are updated.

system volume The volume that contains the hardware-specific files that are needed to load Windows on x86-based computers with a basic input/output system (BIOS). The system volume can be, but does not have to be, the same volume as the boot volume. See also volume.

Systems Management Server (SMS) A Microsoft product that includes inventory collection, software deployment, and diagnostic tools. SMS automates the task of upgrading software, allows remote problem solving, provides asset management information, and monitors software usage, computers, and networks.

SYSVOL A shared directory that stores the server copy of the domain's public files, which are replicated among all domain controllers in the domain. See also domain; domain controller.

T

Terminal Services The underlying technology that enables Remote Desktop, Remote Assistance, and Terminal Server.

topology The physical layout of computers, cables, switches, routers, and other components of a network. *Topology* also refers to the underlying network architecture, such as Ethernet or Token Ring.

In Active Directory replication, the set of connections that domain controllers use to replicate information among themselves.

See also Active Directory replication; domain controller.

transform A custom script created to customize the behavior of an installation by directly modifying the setup script and without repacking the application.

Transmission Control Protocol/Internet Protocol (TCP/IP) A set of networking protocols widely used on the Internet that provides communications across interconnected networks of computers with diverse hardware architectures and various operating systems. TCP/IP includes standards for how computers communicate and conventions for connecting networks and routing traffic. See also Internet Protocol (IP).

U

unicast An address that identifies a specific, globally unique host.

Unicode A character encoding standard developed by the Unicode Consortium that represents almost all of the written languages of the world. The Unicode character repertoire has multiple representation forms, including UTF-8, UTF-16, and UTF-32. Most Windows interfaces use the UTF-16 form.

Uniform Resource Locator (URL) An address that uniquely identifies a location on the Internet. A URL for a World Wide Web site is preceded by *http://*, as in the fictitious URL *http://www.example.microsoft.com*. A URL can contain more detail, such as the name of a page of hypertext, usually identified by the file name extension .html or .htm.

Universal Naming Convention (UNC) A convention for naming files and other resources beginning with two backslashes (\), indicating that the resource exists on a network computer. UNC names conform to the *\\servername\sharename* syntax, where *servername* is the server's name and *sharename* is the name of the shared resource. The UNC name of a directory or file can also include the directory path after the share name, by using the following syntax:
\\servername\sharename\directory\filename.

URL See definition for Uniform Resource Locator (URL).

User Datagram Protocol (UDP) A transport layer protocol that offers a connectionless datagram service that guarantees neither delivery nor correct sequencing of delivered packets (much like Internet Protocol (IP)), but provides a payload checksum and upper layer protocol identification that uses source and destination ports. See also Internet Protocol (IP); Transmission Control Protocol/Internet Protocol (TCP/IP).

user profile A file that contains configuration information for a specific user, such as desktop settings, persistent network connections, and application settings. Each user's preferences are saved to a user profile that Windows uses to configure the desktop each time a user logs on.

user rights Tasks that a user is permitted to perform on a computer system or domain. There are two types of user rights: privileges and logon rights. An example of a privilege is the right to shut down the system. An example of a logon right is the right to log on to a computer locally. Both types are assigned by administrators to individual users or groups as part of the security settings for the computer. See also domain.

user rights policy Security settings that manage the assignment of rights to groups and user accounts. See also user rights.

V

virtual IP address An IP address that is shared among the hosts of a Network Load Balancing cluster. A Network Load Balancing cluster might also use multiple virtual IP addresses, for example, in a cluster of multihomed Web servers. See also IP address; Network Load Balancing cluster.

virtual private network (VPN) The extension of a private network that encompasses encapsulated, encrypted, and authenticated links across shared or public networks. VPN connections typically provide remote access and router-to-router connections to private networks over the Internet. See also authentication; remote access.

volume An area of storage on a hard disk. A volume is formatted by using a file system, such as file allocation table (FAT) or NTFS, and has a drive letter assigned to it. You can view the contents of a volume by clicking its icon in Windows Explorer or in My Computer. A single hard disk can have multiple volumes, and volumes can also span multiple disks. See also NTFS file system.

W-Z

wide area network (WAN) A communications network connecting geographically separated locations that uses long-distance links of third-party telecommunications vendors. See also local area network (LAN).

Windows Installer An operating system service that enables the operating system to manage the installation process. Windows Installer technologies are divided into two parts that work in combination: a clientside installer service (Msiexec.exe) and a package (.msi) file. Windows Installer uses the information contained within a package file to install the application.

Windows Internet Name Service (WINS)

A Windows name resolution service for network basic input/output system (NetBIOS) names. WINS is used by hosts running NetBIOS over TCP/IP (NetBT) to register NetBIOS names and to resolve NetBIOS names to Internet Protocol (IP) addresses. See also IP address; network basic input/output system (NetBIOS).

Windows Management Instrumentation (WMI)

A management infrastructure in Windows that supports monitoring and controlling system resources through a common set of interfaces and provides a logically organized, consistent model of Windows operation, configuration, and status.

Windows Management Instrumentation filter

A query that is based on Windows Management Instrumentation (WMI) and used to filter the effect of a Group Policy object (GPO). WMI filters are written in WMI Query Language (WQL) and are evaluated on the target computer or user. If the filter evaluates to true, then the GPO is applied. Otherwise, the GPO is not applied. WMI filters are useful for exception management. See also Group Policy Management console (GPMC); Group Policy object (GPO).

Windows Update A Microsoft-owned Web site from which Windows users can install or update device drivers. By using an ActiveX control, Windows Update compares the available drivers with those on the user's system and offers to install new or updated versions.

WINS See definition for Windows Internet Name Service (WINS).

WMI filter See definition for Windows Management Instrumentation filter.

Index

Special Characters

32-bit applications 367

64-bit applications 367

A

Access Control Entry (ACE) 141

Access Control List (ACL) 254

account lockout policies 183–184

account security policies 183–184

Active Directory

 See *also* Group Policy; IntelliMirror

 described 8

 desktop management tools 15

 IPSec policies 164

 local infrastructure deployment 447–451

 non-Active Directory computers 340

Active Directory Migration Tool (ADMT) 256

Add the Administrator security group to the roaming user
 profile share policy 302

.adm files 100–102

administration

 configuration management requirements 28

 Group Policy objects 64, 93

 Group Policy 56, 88–93

 software restriction policies and 188

 Software Update Services 204, 219

administrative install 378

Administrative Templates extension 9

Administrative Tools Pack 459, 469

ADMT (Active Directory Migration Tool) 256

advertisement scripts 383

all user policies 80–81, 463–466

Allow processing across a slow network connection
 policy 98, 99

Always use local ADM files for Group Policy Object Editor
 policy 102

Always wait for the network at computer startup and
 logon policy 297

application compability for updates 201

Application Data for user profiles 270

application deployment See software deployment

application migrations 249

application server shares 455

Application Server 440

application-specific settings 249

Apply Group Policy permissions 72, 75, 89

approving SUS updates

 See *also* SUS synchronization

 list of 222

 logs 223

 overview 222–224

 revised content 215

assigning software 387–390

audit policy settings 185

authentication

 IPSec 163–166

 setting up 463

 wireless networks 178, 189, 192–193

auto-install by file activation option 389

automatic policy refreshes 67

automatic synchronizations 209

automatic system updates See SUS (Software Update
 Services)

automatic update approvals 215

Automatic Updates

 Active Directory environments 230

 configuring 229–233, 463

 deploying 226–228

 described 200

 Group Policy 230

 non-Active Directory environments 231

 overview 202

 version upgrades 228

auto-populating migration tables 142

B

- backups
 - Group Policy objects 73, 108–114
 - Group Policy staging 122
 - servers 476–477
- bandwidth
 - requirements 277–278
 - software deployment and 372
- basic services *See* SLAs (service level agreements)
- block filtering 163

C

- cache
 - encryption 315
 - local workstation storage 275
 - Offline Files 321
 - roaming user profiles 335
- categorizing applications 392
- centralized automation 245–247
- certificates 254, 414
- Change Domain Controller function 95
- changed Group Policy settings 66–67, 103–104
- child servers 209
- classifying applications 392
- client components *See* SUS client components
- client operating systems 444–446
- client support for updates 202
- client-side extensions 98–100
- collecting user state
 - centralized automation 245–247
 - manual migrations 243–245
 - overview 241–242
 - scripts 244–247
 - user-driven migration 247
- command prompt
 - Group Policy Modeling 107
 - policy refreshes 104
 - restricting access 80
- compatibility for updates 201
- comparing registry images 255
- Compatws.inf template 170
- complete application installations 389
- compression, roaming user profiles 296
- computer migration *See* user state migration
- computer multiple user configuration 20
- computer patch updates *See* SUS (Software Update Services)
- computer replacements
 - configurations 43
 - examples 14
 - managed desktops for 288
 - Remote Installation Services 272
- computer roles
 - evaluating 20–22
 - mapping configurations to 37–43
- computer security policies *See* security policy
- computer service evaluations 274
- computer settings management 34
- computer software restrictions 413–418
- computer-assigned applications 351, 388
- configuration management
 - additional resources 48
 - administrative requirements 28–31
 - corporate policies 24
 - deployment plans 16
 - deployment process 4–6
 - designing 37–43
 - desktop environment 19
 - examples 11–16
 - need assessments 18
 - network requirements 24–28
 - overview 1–4
 - roles 20–22, 37–43
 - scope 17, 44
 - security requirements 23
 - software 35–36
 - staging deployment 48
 - storage requirements 24–28
 - technologies listed 7–11
 - testing 45–48
- configuring users and computers *See* Group Policy
- connectivity
 - See also* configuration management; slow links
 - roaming user profiles 291
 - Software Update Services 204, 206

- container Group Policy object tasks 90
- converting Group Policy object values 113–114
- CopyGPO.wsf 153
- copying GPOs 111, 123, 152–153
- corporate policies 24, 63
- corporate standard GPOs 80
- cost calculations for migration 250
- CreateEnvironmentFromXML.wsf 131–135
- CreateMigrationTable.wsf 147
- CreateXMLFromEnvironment.wsf 131–135
- critical security rating 200
- cross-forest GPO importing 122
- cryptography
 - Folder Redirection 312, 315
 - IPSec 163–166
 - Offline Files 322
 - security policy 167
 - user state migration 254
- Custom permissions 89
- custom security templates 169
- custom services *See* SLAs (service level agreements)
- customized home page URLs 14
- customizing .inf files 240, 253
- customizing User State Migration Tool 240
- customizing Windows Installer packages 359

D

- DACL (Discretionary Access Control List) 111
- data backups 476–477
- data management options 31
- data migration *See* user state migration
- data-entry users 21, 42
- DC security.inf template 170
- DC *See* domain controllers (DC)
- decryption 254
- default
 - disk quota limits 337
 - Folder Redirection settings 308
 - Group Policy update intervals 100
 - migration files and settings 239
 - Offline Files state 331
 - policy restoration 73

- default (*continued*)
 - roaming user profiles 306
 - security settings 175
 - slow link settings 96
 - slow-link thresholds 61, 277
 - SUS settings 212
- Default Domain Controller GPO 73, 167, 185
- Default Domain GPO 73, 167, 183–184
- delegating administrative authority 59, 88–93
- Delete cached copies of roaming profiles policy 285, 296
- desktop environment assessments 19
- desktop configurations *See* managed desktop configurations
- detecting slow links 97
- DFS (Distributed File System)
 - configuring 372
 - described 371
 - root shares 453–454
 - software distribution point servers 377
- dictionary objects *See* metadata
- directory-based configuration management *See* IntelliMirror
- Diruse.exe 275
- disabling
 - GPO configuration settings 85
 - policy settings 70
 - roaming user profiles 304
 - script mappings 217
- Disallowed security level 186–188
- disapproving SUS updates 223
- disconnected file access *See* Offline Files
- Discretionary Access Control List (DACL) 111
- disk partitions 437, 443
- disk quotas
 - administrative requirements 336
 - configuring 338–339
 - described 10, 272
 - Group Policy 336–338
 - options 339
 - overview 334, 336–338
 - recommendations 336
 - roaming user profiles 296

- disk quotas (*continued*)
 - setting up 466
 - user preparation 292
- disk space
 - See also Folder Redirection
 - allocations 24–28
 - over-allocating 336–338
 - roaming user profiles 296
 - storage requirements 275–276
- displaying SUS synchronization logs 221
- displaying SUS update information 222
- Distributed File System See DFS (Distributed File System)
- distribution point servers
 - configuring 378–380
 - overview 377
- distribution points 218, 227
- DLL checking 188
- DNS (Directory Name Service) 129
- DNS (Domain Name System) 213, 437
- Do not apply during periodic background processing policy 99
- domain controllers (DC)
 - configuring 437–441
 - deploying 437
 - desktop management 20
 - drive partition formatting 443
 - GPO editing 94
 - GPO links 73
 - recommendations 433, 435
 - security policies 185
 - slow links 61
 - specifying 95
 - time synchronization 442
- domains
 - GPO backups 122
 - GPO copying 123
 - GPO links 73, 85
 - GPO tasks 90
 - Group Policy synchronization 131–135
 - migration 256
 - names 116
 - remote access 291

- domains (*continued*)
 - security policy 167, 183–184
 - software targeting 384
- drive partition formatting 443

E

- Edit permissions 89
- Edit/Delete/Modify Security permissions 89
- editing GPOs 84, 94
- EFS (Encrypting File System)
 - Folder Redirection 312
 - Offline Files 322
 - roaming user profiles 296
 - user state migration 254
- e-mail, user state migration and 249
- encapsulating packages 360
- Encrypt the offline files cache policy 316
- encryption
 - Folder Redirection 312, 315
 - IPSec 163–166
 - Offline Files 322
 - security policy 167
 - user state migration 254
- Enforced option 69–71
- evaluating current environment
 - desktop management 19
 - overview 18
 - roles 20–22
- events
 - security policy 168
 - Software Update Services 223
- exception management 76
- Exclude directories in roaming profile policy 276, 297
- excluding folders from user profiles 276
- excluding local administrators 188
- external domain users 92
- external time sources 442

F

- fast logon enhancement 297
- File Replication System (FRS) 371

- files
 - See also Offline Files; Synchronization Manager; user state migration
 - name collisions 253
 - relocations 253
 - user profiles 269
- Files and Settings Transfer Wizard
 - ACLs 254
 - encryption 254
 - overview 238
 - user-driven migrations 247
- filters
 - Group Policy objects 75–79
 - IPSec 163–166
- firewalls
 - shared resources 330
 - Software Update Services 206
- first time log ons 12
- folder migration See user state migration
- Folder Redirection
 - default settings 308
 - described 10, 270
 - encryption 312, 315
 - Group Policy guidelines 312
 - home directories 310, 318
 - log files 319
 - logging on after 278
 - My Documents 309, 318
 - non-Active Directory computers 340
 - Offline Files 309, 311
 - Outlook 311
 - overview 307
 - quotas 335
 - recommendations 308–312
 - roaming user profiles 295
 - security 314–319
 - setting up 463
 - special folders 317
 - Start Menu 311
 - user preparation 291
- folders for user profiles 269
- forced application removals 412

- forcing synchronization 323
- formats
 - drive partitions 443
 - migration tables 146
- Free Text or SID 142
- FRS (File Replication System) 371
- full synchronization 320

G

- GPMC (Group Policy Management Console)
 - described 8
 - domain controllers 94
 - GPO backups 108–110, 122
 - GPO copying 111, 123, 152–153
 - GPO creation 84
 - GPO importing 122, 154–156
 - GPO links 472
 - GPO migration 113–114
 - Group Policy Modeling 105
 - installing 57, 448
 - migration tables 124, 140–147
 - overview 56–57
 - scripts 117
 - software deployment troubleshooting 420–425
 - staging tools 122–125
 - synchronization 130–135
- GPOs (Group Policy objects)
 - administration 64, 93
 - backups 73, 108–114, 122, 477
 - copying 111, 123, 152–153
 - creating 83–87, 91–92, 463
 - delegating authority 88–93
 - disabling settings 85
 - editing 84, 94
 - filtering 75–79
 - importing settings 112
 - importing 122, 133, 154–156
 - linking 73–75, 84, 472
 - migrating 113–114
 - migration tables 124, 140–147
 - number needed 72–79

GPOs (Group Policy objects) *(continued)*

- OU structure 59–61
- overview 52
- permissions 89
- production deployment 148–156
- replication 149
- restoring 110
- security policy 167
- service level agreements 62
- software deployment troubleshooting 420–425
- software restriction policies 416
- software targeting 381–383
- synchronization 130–135
- troubleshooting 115

Gpresult.exe 107

Gptool.exe 61

gpupdate command 67, 474

granting profile share permissions 301

Group Policy

- See also GPMC (Group Policy Management Console);
Group Policy planning; Group Policy staging;
managed desktop configurations; security policy

- additional resources 117
- administration 56, 88–93
- application scope 45
- Automatic Updates 227, 230
- changed settings interval 66–67, 103–104
- configuration management and 4
- described 8
- disk quotas 336–338
- examples 53
- Folder Redirection 312
- implementation process 54
- inheritance 68
- loopback processing 87
- maintaining 115–117
- Offline Files 324–329
- overview 51–53
- processing order 70
- roaming user profiles 296–300

Group Policy *(continued)*

- slow link modifications 277
- software deployment 349–351, 381–390, 420–425
- software upgrades 411
- testing 136–139
- tools 56–57

Group Policy containers 100

Group Policy Creator Owners security group 91

Group Policy deployment

- administration 88–93
- backing up 108–114
- client-side extensions 99–100
- domain controllers 94
- GPO creation 83–87, 91–92
- operational guidelines 93
- overview 82–83
- refresh intervals 103–104
- settings evaluation 105–108
- slow links 95–98
- stored information 100–102

Group Policy design

- all users 80–81
- GPO quantity 72–79
- overview 68
- preparation 55
- process 54
- scope 70

Group Policy Management Console See GPMC (Group Policy Management Console)

Group Policy MMC snap-in See Group Policy Object Editor

Group Policy Modeling

- Group Policy testing 136–139
- linked GPOs 472
- settings evaluation 105–108
- troubleshooting deployments 420–425

Group Policy Modeling Wizard 105–106, 138

Group Policy Object Editor 94

Group Policy objects See GPOs (Group Policy objects)

- Group Policy planning
 - interoperability 65–67
 - objectives 63–64
 - operational guidelines 64
 - OU structure 59–61
 - overview 58
 - refresh intervals 66–67
 - service level agreements 62
 - software installations 68
- Group Policy Refresh Interval for Computers policy 67, 103
- Group Policy Refresh Interval for Domain Controllers policy 67, 103
- Group Policy Refresh Interval for Users policy 67, 103
- Group Policy Results
 - Group Policy testing 136–139
 - settings evaluation 105–108
 - software deployment 423
 - testing deployment 474
- Group Policy Results Wizard 115, 138, 180
- Group Policy Slow Link Detection policy 61, 97, 99, 277, 283
- Group Policy staging
 - additional resources 156
 - creating 126–129
 - GPO importing 133
 - hardware requirements 128
 - migration tables 141–147
 - options 127–128
 - overview 119–120
 - populating domain 134
 - preparing 129
 - process 121
 - production deployment 148–156
 - production examples 150–156
 - production precautions 149
 - production preparation 140–147
 - synchronization 130–135
 - technology background 122–125
 - testing 136–139
 - verification checklist 150
 - XML format files 131–135

- Group Policy template 100
- group security policies *See* security policy

H

- hardware
 - Automatic Updates 203
 - Group Policy staging 128
 - SUS server component 202
- hash rules 414
- hierarchies, Group Policy settings 59
- high performance users 21
- highly managed configurations 37
- highly managed desktops 285
- Hisec*.inf templates 173–174
- HKEY_CURRENT_USER 255
- home directory redirection 310, 318
- home page URLs 14
- HTTPS 219

I-K

- identifying computers, user state migration 246
- identifying migration content
 - applications 249
 - cost calculations 250
 - data 248
 - overview 248
 - user settings 249–251
- IEEE 802.1X authentication 189–193
- Ignore Language parameter 386
- IIS Lockdown tool 204, 216
- IIS 201, 216
- immediate SUS synchronizations 221
- immediate updating, linked GPOs 474
- ImportGPO.wsf 155
- importing GPOs 122, 133, 154–156
- importing GPO settings 112
- importing security templates 182
- Inf Commands.doc file 239
- .inf files 239, 253
- inheritance, Group Policy 68, 70, 80
- in-place application upgrades 419
- Install this application at logon option 374

installing operating systems remotely 36, 272
installing software updates 222

IntelliMirror

See also managed desktop configurations
additional resources 48
administrative requirements 28–31
corporate policies 24
deployment plans 16
deployment process 4–6
design considerations 37–43
desktop environment 19
examples 11–16
features 7
need assessments 18
network requirements 24–28
overview 1–4
roles 20–22, 37–43
scope 17, 44
security requirements 23
software 35–36
staging deployment 48
storage requirements 24–28
technologies listed 7–11
testing 45–48
user state management 266

internally synchronized servers 209

international considerations 201, 215, 386

Internet Explorer

configuration management 9
policy settings 4

Internet zone rules 415

interoperability, Group Policy 65

intranet 206, 214

IP addresses 435, 445

IP filters 163–166

IPSec (IP Security Protocol)

applying changes 165
described 302
designing policies 163–166

ISAPI handlers 217

job-based desktop configurations 20

Kerberos

account policies 183–184
described 302

kiosk workstations 41

knowledge users 21

L

lab testing 259

language support 201, 215, 386

LAN-router connections 436

large-size organizations, software deployment 207–210

LGPOs (local Group Policy objects) 16

lightly managed configurations 38

lightly managed desktops 286

Limit profile size policy 291, 297

link speed

domain controller locations 61
measuring 95
specifying Group Policy for 96–98

linking GPOs 73–75, 84, 472

load balancing 210, 220

Loadstate.exe 239

local Group Policy objects (LGPOs) 16

local infrastructure 447–451

local security policies 185

local user profiles 10, 270, 304

local workstation storage 275

locales, SUS synchronization 215

locally hosted updates 214

lockout policies 183–184

log wrapping 168

logging on

examples 12–14
fast logon enhancement 297
Folder Redirection and 278
GPO quantity and 72
roaming user profiles 290, 296

- logs
 - Folder Redirection 319
 - roaming user profiles 307
 - security policy 168
 - SUS synchronization 221, 224
 - SUS update approvals 223
- loopback processing
 - applying user settings 20, 87
 - Group Policy staging 139
 - roaming user profiles 297
- low-level GPO permissions 89
- low security rating 200

M

- MAC (media access control) 246
- major application upgrades 410
- managed desktop configurations
 - See also user state management
 - highly managed desktops 285
 - lightly managed desktops 286
 - mobile users 281–284
 - multi-user desktops 286–287
 - new users 280
 - overview 278
 - replacing computers 288
- managed environments
 - See also simple managed environment
 - additional resources 48
 - administrative requirements 28–31
 - corporate policies 24
 - deployment plans 16
 - deployment process 4–6
 - designing 37–43
 - desktop environment 19
 - examples 11–16
 - need assessments 18
 - network requirements 24–28
 - overview 1–4
 - roles 20–22, 37–43
 - scope 17, 44
 - security requirements 23
 - software 35–36
 - staging deployment 48
 - managed environments *(continued)*
 - storage requirements 24–28
 - technologies listed 7–11
 - testing 45–48
 - mandatory user profiles 10, 270
 - manual migration table data entry 146
 - manual migrations 243–245
 - manual policy refreshes 67
 - manual synchronizations 209
 - manually created upgrade relationships 411
 - mapping
 - ACEs 141
 - security principals 141
 - source and destination values 113–114
 - UNC paths 124, 141
 - maximum profile quotas 335
 - maximum profile size 276
 - MaxNoGPOListChangesInterval 100
 - measuring link speed 95
 - media access control (MAC) 246
 - medium-size organizations, software deployment 207–210
 - member servers 20
 - merge loopback mode 87, 139
 - Merge mode 298
 - message digests 414
 - metadata 214
 - Microsoft Office 455, 459, 463
 - Migapp.inf 239
 - migrating applications to managed environment 400–404
 - migrating Group Policy objects 113–114
 - migrating user state
 - additional resources 260
 - centralized automation 245–247
 - collection methods 241–242
 - data 248, 253
 - domains 256
 - file relocations 253
 - identifying content 248
 - manual 243–245
 - overview 235–237
 - planning 251

migrating user state *(continued)*

- registry 255
- scheduling 257
- scripts 244–247
- security 253–255
- storage 252–253
- system deployment methods and 241
- testing 258–259
- tools 238–240
- user preparation 257
- user settings 249–251
- user-driven 247

migration tables

- auto-populating 142
- formats 146
- GPOs 113–114
- manual data entry 146
- mapping types 141
- object types 142
- overview 124, 141
- scripts 147

Migsys.inf 239

Miguser.inf 239

minor application upgrades 408

mixed environments, Group Policy 65

mobile users

- configuring 284
- managed configurations for 39, 281–284
- management features 283
- need assessment 22
- policies for 470
- software installations 282
- synchronization 282

moderate security rating 200

MOF (Microsoft Operations Framework) 2

monitoring SUS servers 223

MSF (Microsoft Solutions Framework)

- described 2
- team model 17

.msi files

- 64-bit applications 367
- customizing 359
- described 354
- examples 360
- overview 359
- reauthoring applications 363–364
- repackaging applications 355, 368–369
- vs. .zap files 364

.msp files 407

MTE (Migration Table Editor) 111, 125, 141–147

multilingual considerations 201, 215, 386

multiple domain controllers 433

multiple servers, Software Update Services 201, 207–210, 220

multiple user migration *See* user state migration

multiple users accessing distributed software 376

multi-user configurations 20, 40

multi-user desktops 286–287

My Documents

- redirecting 309, 318
- user profiles 270

My Pictures 270

N

names

- file relocations 253
- name services integration 129
- UNC 377

NAT (Network Address Translation) 435

native Windows Installer packages

- 64-bit applications 367
- customizing 359
- described 354
- examples 360
- overview 359
- reauthoring applications 363–364
- repackaging applications 355, 368–369
- vs. .zap files 364

- net start policyagent command 165
- net stop policyagent command 165
- Netsh IPsec context 164
- network adapters, user state migration 246
- network bandwidth
 - requirements 24–28, 277–278
 - software deployment and 372
- network capacity 372
- network file synchronization *See* synchronization
- network infrastructure
 - client operating systems 444–446
 - domain controllers 437–443
 - evaluating 372–373
 - physical network 436
 - setup steps 435
 - Windows XP Professional 444–446
- network keys 190
- network load balancing 210, 220
- network migration considerations 257
- network requirements 24–28
- network testing 45–48
- network traffic assessments 24–28
- new user desktop configurations 280
- new user log ons 12
- NLB (network load balancing) 210, 220
- No Override option *See* Enforced option
- non-Active Directory computers 340
- non-Active Directory environments 15
- notifications, Software Update Services 229
- notifying file conflicts *See* Synchronization Manager
- Notssid.inf template 174
- NTFS
 - described 303
 - Folder Redirection 314–319
 - roaming user profiles 296, 301
 - security policy 167
 - shared resources 330

O

- Offline Files
 - available files and folders 320
 - caching 321
 - configuring 331–333, 463
 - described 10, 271
 - encryption 322
 - examples 13
 - Folder Redirection 309, 311
 - Group Policy guidelines 324–329
 - overview 320
 - policy settings 324–329
 - recommendations 320–324
 - roaming user profiles 296
 - security 329–330
 - shared resources 329–330
 - synchronization 323, 333
 - Terminal Services 322
 - user preparation 291
- on-demand application installations 390
- Only allow local user profiles policy 304
- open system authentication 189
- operating systems
 - See also* user state migration
 - remote configurations 4, 11
 - remote installations 36, 272
 - roaming user profiles 295
 - Software Update Services 202
- Operations Master token 95
- optional application removals 412
- organization management requirements 17
- OU (organizational units)
 - administrator isolation 75
 - corporate standards 81
 - creating 448
 - described 54
 - designing 59–61
 - GPO links 74, 85
 - GPO tasks 90
 - hierarchy 44

Outlook, folder redirection 311
 over-allocating disk space 336–338
 overriding Group Policy objects 70

P

packages 214, 222
 packaging software
 64-bit applications 367
 native Windows Installer packages 359–364
 overview 357
 repackaging applications 368–369
 .zip files 364–366
 parallel deployments 241, 245
 parent servers 209
 passwords
 account password policies 183–184
 shared resources 330
 patches
 See also SUS (Software Update Services)
 comparing deployment options 199–200
 examples 418
 overview 407
 path rules 414
 PDC emulators 94, 442
 per-container Group Policy object tasks 90
 performance, software deployment 375, 393–397
 permissions
 Folder Redirection 314–319
 Group Policy delegations 88–93
 Group Policy objects 75, 89
 IPSec 163–166
 roaming user profiles 301
 Security Filtering 72
 shared resources 329–330
 software distribution point servers 379
 permit filtering 163
 persisting security settings 168
 physical network setup 436
 pilot testing 47, 194, 259, 290, 393–397
 policy refresh intervals 66–67, 103–104
 policy settings *See* Group Policy
 polling IPSec changes 165
 polling SUS servers 229
 populating Group Policy staging domain 134
 portable computer log ons 13
 precedence
 Group Policy 70, 75
 security policy 167
 software restriction rules 418
 software restrictions 186
 wireless network policies 179–180
 predefined security templates
 recommendations 175
 types 169–174
 preferred wireless networks 192–193
 Prevent access to the command prompt policy 80
 Prevent access to the registry editing tools policy 80
 Prevent Roaming Profile changes from propagating to the server policy 304
 primary domain controller (PDC) emulator 442
 priority processing, Group Policy 70, 74
 Process event if the Group Policy objects have not changed policy 100
 process users 21
 processing order, Group Policy 70, 74
 processor serial numbers 246
 production environment staging *See* Group Policy staging
 profile quotas
 assigning 335
 described 271
 overview 334
 user preparation 292
 profiles *See* roaming user profiles; user profiles
 proof of concept testing 46
 proxy servers 212
 public updates Web site *See* Windows Updates
 publishing software 391–392

Q

- quick synchronization 320
- quotas
 - described 271
 - disk quotas 336–339
 - overview 334
 - setting up 466
 - user preparation 292
 - user profiles 335

R

- Read (from Security Filtering) permissions 89
- Read permissions 72, 75, 89
- reauthoring applications 363–364
- Recycle Bin 310
- Redircomp.exe 44, 450
- Redirect to home folder policy 309
- redirecting Automatic Updates 231
- redirecting folders
 - default settings 308
 - described 10, 270
 - encryption 312, 315
 - Group Policy guidelines 312
 - home directories 310, 318
 - log files 319
 - logging on after 278
 - My Documents 309, 318
 - non-Active Directory computers 340
 - Offline Files 309, 311
 - Outlook 311
 - overview 307
 - quotas 335
 - recommendations 308–312
 - roaming user profiles 295
 - security 314–319
 - server shares 457
 - setting up 463
 - special folders 317
 - Start Menu 311
 - user preparation 291
- redirecting Users and Computers containers 44
- Redirusr.exe 44, 450
- refresh intervals 66–67, 103–104
- refreshing security settings 176
- registered file types 249
- registry
 - Automatic Updates 231
 - Group Policy 80
 - hive 269
 - path rules 414
 - policy settings 9
 - user state migration 250, 255
- relocating files 253
- relocating registry entries 255
- remote access, user preparation 291
- remote administration
 - configuration management 4, 11
 - network requirements 25–28
 - Software Update Services 219
- remote connection slow links 95, 98
- Remote Installation Services *See* RIS (Remote Installation Services)
- remote log ons 13
- remote operating system installations 36
- remote user need assessments 22
- remote user software deployment 374–376
- Remotely access Group Policy Results data permission 106
- removing
 - cached roaming profiles 336
 - Group Policy for Folder Redirection 312
 - installed applications 412, 419
 - Windows Updates access 230
- renaming domains 116
- repackaging applications 355, 368–369, 411
- replace loopback mode 87, 139
- Replace mode 297
- replacing computers
 - configurations 43
 - examples 14
 - managed desktops for 288
 - Remote Installation Services 272

- replication
 - Group Policy 66–67, 87, 94, 101
 - status information 149
- requirements
 - See also configuration management
 - network 277–278
 - software distribution point servers 377
 - Software Update Services 202
 - storage 275–276
 - user 274
- resolving file conflicts See Synchronization Manager
- resource management requirements 18
- restarting IPsec service 165
- restoring
 - configuration on replacement computers 14, 43
 - default policies 73
 - GPOs 110, 122
- Restricted Groups policy 168
- Restricted/Permitted Snap-ins\Extension snap-ins policy 93
- revised patch content 215
- RIS (Remote Installation Services)
 - See also managed desktop configurations
 - described 11, 272
 - migrating applications 400–404
- roaming user need assessments 22
- Roaming User Profiles
 - See also Folder Redirection
 - configuring 303–307
 - deleting cached profiles 336
 - described 10, 270
 - disabling 304
 - Group Policy guidelines 296–300
 - local profiles 304
 - log files 307
 - operating system versions 295
 - overview 295
 - policies for 467
 - policy settings 300
 - quotas 335
- Roaming User Profiles (*continued*)
 - recommendations 295–296
 - security 300–303
 - server shares 456–457
 - shared computers 14
 - size reductions 276
 - user preparation 290
- roles
 - evaluating 20–22
 - mapping configurations to 37–43
- rolling back deployments 156
- root shares 308
- Rootsec.inf template 174
- router configuration 436
- RSoP data 106
- RSoP logging mode See Group Policy Results
- RSoP planning mode See Group Policy Modeling
- rules
 - software restriction policies 413–418
 - software restriction precedence 186

S

- scaling out SUS deployments 207–210
- scanning tool comparisons 199–200
- Scanstate.exe 239
- scheduling Automatic Updates 229
- scheduling migrations 257
- scheduling synchronizations 221, 333
- scripts
 - advertisement 383
 - centralized automation 245–247
 - configuration management 4, 9
 - copy deployments 153
 - disabling mappings 217
 - GPMC 56–57, 117
 - import deployments 155
 - manual migrations 244–245
 - migration tables 147
 - non-Active Directory computers 340
 - roaming user profiles 305
 - software upgrades 411
 - synchronization 131

- secedit/refreshpolicy command 67, 104
- Secure Sockets Layer 219
- Secure*.inf templates 171–172
- security
 - See also security policy; SUS security
 - configuration management 3, 9, 23
 - deploying 451
 - Folder Redirection 314–319
 - registry 256
 - roaming user profiles 300–303
 - shared resources 329–330
 - software distribution point servers 379
 - software restriction policies 413–418
 - user state migration 253–255
- Security Configuration Manager 161
- Security Filtering 72, 75
- security identifiers (SIDs) 256
- security policy
 - account policies 183–184
 - additional resources 194
 - changing settings 169, 182–185
 - configuration options 181
 - custom templates 169
 - default settings 175
 - deployment process 159
 - designing 162
 - encryption 167
 - Group Policy 160–161
 - importing templates 182
 - IPSec 163–166
 - local policies 185
 - overview 157–158
 - predefined templates 169–175
 - refreshing settings 176
 - Security Configuration Manager 161
 - settings guidelines 167–169
 - software restrictions 176, 186–188
 - testing 194
 - tools 160–161
 - wireless networks 177–180, 189–193
- security principals 122, 141
- serial numbers 246
- server components (SUS) 201
- server disk storage 275
- Server Message Block (SMB) signing 303
- server roles 441
- server shares 455–457
- service level agreements (SLAs)
 - described 28
 - Group Policy 62
- settings migration See user state migration
- Setup security.inf template 170, 175
- severity ratings 200
- share level permissions
 - Folder Redirection 314–319
 - roaming user profiles 301
- shared computer environments 13
- shared files See Offline Files
- shared folders 452–457
- shared key authentication 189
- shared resource security 329–330
- SIDs (security identifiers) 256
- simple managed environment
 - additional resources 478
 - Administrative Tools Pack 459, 469
 - all user policies 463–466
 - assumptions 432–434
 - backing up 476–477
 - deployment process 431
 - deployment steps 470–478
 - hardware requirements 434
 - local infrastructure 447–451
 - mobile users 470
 - network infrastructure 435–446
 - overview 429–431
 - roaming user profiles 467
 - sample configuration 432–434
 - shared folders 452–457
 - software installation 458–461
 - software requirements 434
 - testing 470–475
 - user state management 462–470

- simulating Group Policy deployment 105–108
- simultaneous migration *See* centralized automation
- simultaneous software deployment access 376
- single-purpose workstations 41
- site Group Policy object links 73, 85, 86
- site Group Policy object tasks 90
- site locations, Group Policy 61
- size, profiles 276, 296, 335
- SLAs (service level agreements)
 - described 28
 - Group Policy 62
- slow links
 - domain controller locations 61
 - Group Policy staging 139
 - measuring 95
 - software deployment and 373, 375
 - specifying Group Policy for 96–98
 - thresholds 277
- Slow network connection timeout for user profiles policy 97
- small application upgrades 408
- SMB (Server Message Block) signing 303
- SMS (Systems Management Server)
 - See also* SMS with SUS Feature Pack
 - configuration management 15
 - software deployment 347, 374
 - user state migration 246
- SMS with SUS Feature Pack
 - described 200
 - vs. SUS 199–200
- software deployment
 - additional resources 426
 - assigning software 387–390
 - available to users 376, 398–399
 - categorizing applications 392
 - computer-assigned applications 351, 388
 - distribution point servers 377–380
 - Group Policy 349–351, 381–390
 - maintaining after 405
 - software deployment (*continued*)
 - migrating to managed environment 400–404
 - network infrastructure 372–373
 - options 346–348
 - overview 343–345, 370–371
 - packaging 357–369
 - patches 407, 418
 - performance issues 375
 - preparing 352–356
 - publishing software 391–392
 - reauthoring applications 363–364
 - remote users 374–376
 - removing applications 412, 419
 - repackaging applications 368–369
 - restriction policies 413–418
 - targeting 381–392
 - testing 393–397
 - troubleshooting 420–425
 - upgrading applications 408–411, 418–420
 - user requirements 372, 380
 - user-assigned applications 351, 387–392
 - software distribution point servers
 - configuring 378–380
 - overview 377
 - Software Installation Settings files *See* .zap files
 - software installations 68, 282, 458–461
 - software life cycles 405
 - software management options 35–36
 - software restriction policies 176, 186–188, 413–418
 - Software Update Services *See* SUS (Software Update Services)
 - special folder redirection 317
 - SSL (Secure Sockets Layer) 219
 - staged configuration management deployments 48
 - staged SUS deployments
 - described 201
 - scaling out 207–210
 - testing 225

- staged user state migrations 259
- staging Group Policy deployments
 - additional resources 156
 - creating 126–129
 - described 83
 - GPO importing 133
 - hardware requirements 128
 - migration tables 141–147
 - options 127–128
 - overview 119–120
 - populating domain 134
 - preparing 129
 - process 121
 - production deployment 148–156
 - production examples 150–156
 - production precautions 149
 - production preparation 140–147
 - synchronization 130–135
 - technology background 122–125
 - testing 136–139
 - verification checklist 150
 - XML format files 131–135
- stand-alone Migration Table Editor 142
- Standard User Policy GPOs 80
- Start Menu redirection 311
- stationary users 21
- statistics, Automatic Updates 231
- status information
 - network performance 97
 - SUS approvals 222
- stopping IPSec service 165
- storage requirements
 - determining 24–28, 275–276
 - user state migration 252–253
- storing Group Policy information 100–102
- storing user data in managed environment 268
- storing user settings in managed environment 269
- SUS (Software Update Services)
 - See also Automatic Updates; SUS deployments; SUS server components
 - additional resources 233
 - SUS (Software Update Services) (*continued*)
 - administering 219
 - application compability 201
 - approving updates 222–224
 - connectivity 206
 - described 11, 200
 - IIS 216
 - installing 460
 - language support 201, 215
 - network load balancing 210, 220
 - overview 198
 - patches 347, 408
 - related information 197
 - vs. SMS with SUS Feature Pack 199–200
 - Windows updates supported 201
 - SUS client components
 - Active Directory environments 230
 - configuring 229–233
 - deploying 226–228
 - described 200
 - Group Policy 230
 - non-Active Directory environments 231
 - overview 202
 - version upgrades 228
 - SUS deployments
 - Automatic Updates 226–233
 - comparing options 199–200
 - described 198
 - designing 205–210
 - scaling out 207–210
 - server configuration 212–217
 - server installations 211
 - staging content 225
 - SUS security
 - administration 219
 - IIS 216
 - overview 204
 - severity ratings 200

- SUS server components
 - administering 219
 - configuring 212–217
 - default settings 212
 - deployment design 205–210
 - deployment process 211
 - distribution points 218
 - installing 212
 - monitoring functionality 223
 - overview 201–202
 - scaling out 207–210
- SUS synchronization
 - data types 214
 - distribution points 218
 - list of approved items 222
 - logs 221, 224
 - multiple servers 209
 - options 221
- synchronization
 - See also* SUS synchronization
 - DC time synchronization 442
 - Folder Redirection 312
 - Group Policy staging 130–135
 - mobile user settings 282
 - Offline Files 10, 13
 - types 320
 - user preparation 291
- Synchronization Manager
 - configuring 333
 - described 271
 - Offline Files 323
 - roaming user profiles 296
 - user options 291
- Synchronize all offline files before logging off policy 324
- Sysdiff.exe 250, 255
- Sysfiles.inf 239
- system backups 476–477
- system migration *See* user state migration
- system updates *See* SUS (Software Update Services)

- Systems Management Server *See* SMS (Systems Management Server)
- Sysvol folder 100

T

- targeting software deployment
 - assigning software 387–390
 - GPOs 381–383
 - multinational users 386
 - need assessments 380
 - options 372
 - publishing software 391–392
 - scaling 384
- task stations 42
- tattooing 169
- templates
 - custom security templates 169
 - importing 182
 - predefined security templates 169–175
 - roaming user profiles 306
 - security 23
- Terminal Services 322, 347, 374
- test user accounts 138
- testing
 - See also* Group Policy staging
 - configuration management designs 45–48
 - Group Policy design 82
 - Group Policy 136–139
 - migration processes 258–259
 - patches 225
 - security policies 194
 - simple managed environment 470–475
 - software deployment 375, 393–397
 - user state management plans 290
- Timeout for dialog boxes policy 291
- tools
 - Group Policy 56–57
 - patch deployment options 199–200
 - security policy 160–161
 - user state migration 238–240

- traffic assessments 24–28
- transferring files and settings *See* user state migration
- transforms 359–362
- transitioning applications to managed environment 400–404
- translating Group Policy object values 114
- translating registry entries 255
- troubleshooting *See* logs
- trust relationships 127–129, 150–156
- Turn off automatic update of ADM files policy 102
- Turn off background refresh of Group Policy policy 103

U

- UNC mapping 122, 141
- UNC names 377
- unicast mode 221
- unlinking Group Policy objects 84, 85
- Unrestricted security level 186–188
- untrusted relationships 154
- update severity ratings 200
- updating software 222
- updating versions *See* synchronization
- Upgrade option 241
- upgrade relationships 411
- upgrading Automatic Updates 228
- upgrading installed applications 408–411, 418–420
- URLs, customized home pages 14
- Urlscan security tool 204, 216
- user account testing 138
- user configurations *See* managed desktop configurations
- user data defined 268
- user data management 31
- user data server shares 456–457
- User Group Policy loopback processing mode policy 87, 297
- user management *See* IntelliMirror
- user preparation 290–292
- user profiles
 - See also* profile quotas
 - excluding folders from 276
 - folders 269
 - management options 32
- user profiles (*continued*)
 - overview 269
 - quotas 271
 - scripts 305
 - size 296
 - types 9
- user requirements
 - determining 274
 - storage 275
- user rights assignment settings 185
- user roles
 - evaluating 20–22
 - mapping configurations to 37–43
- user security policies *See* security policy
- user settings management 32, 269
- user software requirements 372, 380
- user state management
 - See also* Folder Redirection; managed desktop configurations; Offline Files; roaming user profiles
 - additional resources 341
 - assessing requirements 274–278
 - deployment preparation 289
 - feature configuration 293–294
 - implementation process 265
 - non-Active Directory computers 340
 - overview 263–264
 - planning 273–278
 - policies for 462–470
 - quotas 334–339
 - technology background 266–272
 - user preparation 290–292
- user state migration
 - additional resources 260
 - centralized automation 245–247
 - collection methods 241–242
 - data 248, 253
 - domains 256
 - file relocations 253
 - identifying content 248
 - manual 243–245
 - overview 235–237

- user state migration (*continued*)
 - planning 251
 - registry 255
 - scheduling 257
 - scripts 244–247
 - security 253–255
 - storage 252–253
 - system deployment methods and 241
 - testing 258–259
 - tools 238–240
 - user preparation 257
 - user settings 249–251
 - user-driven 247
- user training and support 47
- user-assigned applications 351, 387–392
- user-driven migrations 247
- USMT (User State Migration Tool)
 - ACLs 254
 - data management 253
 - described 11
 - domain migrations 256
 - encryption 254
 - overview 239–240
 - registry 255

V

- version control *See* Synchronization Manager
- versions, Group Policy interoperability 65
- Vertias WinInstall LE 369
- viewing registered file types 249
- viewing security templates 169
- viewing wireless network settings 180
- virus protection 389, 413, 416, 419, 425

W-Z

- WebDAV 375
- WEP (Wired Equivalent Privacy) key 179
- Windows Installer packages
 - See also* managed desktop configurations
 - 64-bit applications 367
 - customizing 359
 - examples 360

- Windows Installer packages (*continued*)
 - options 352–356
 - overview 357–359
 - reauthoring applications 363–364
 - repackaging applications 355, 368–369
 - upgrades 410–411
 - vs. .zap files 364
- Windows Update Synchronization Service 201
- Windows Updates
 - See also* SUS (Software Update Services)
 - described 199
 - removing access 230
 - SUS synchronization from Web site 214
- Windows XP Professional 444–446
- WINS (Windows Internet Name Service) 129
- wipe-and-load deployments 241, 244
- wireless network policies 177–180, 189–193
- WMI filters
 - delegating 92
 - Group Policy objects 76–79
- WMI Query Language queries (WQL) queries 77
- WSH (Windows Script Host) scripts 131
- XML 131–135
- .zap files
 - creating 364
 - described 354
 - examples 366
- zone rules 415