

# **Microsoft® Windows® Server 2003 Deployment Kit**

## **Automating and Customizing Installations**

**A Resource Kit Publication**

**William Gruber, Sandra Faucett, Greg Gille, Jim Bevan, Deborah R. Jay,  
Chris McKitterick**

Microsoft Corporation

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

<b>CHAPTER 1</b>	<b>Choosing an Automated Installation Method .....</b>	<b>1</b>
<b>CHAPTER 2</b>	<b>Designing Unattended Installations .....</b>	<b>19</b>
<b>CHAPTER 3</b>	<b>Designing Image-based Installations with Sysprep .....</b>	<b>91</b>
<b>CHAPTER 4</b>	<b>Designing RIS Installations .....</b>	<b>161</b>
<b>CHAPTER 5</b>	<b>Migrating User State .....</b>	<b>295</b>
<b>GLOSSARY</b>	<b>.....</b>	<b>323</b>
<b>INDEX</b>	<b>.....</b>	<b>329</b>



# Contents

<b>Introduction .....</b>	<b>xiii</b>
Deployment Kit Compact Disc .....	xiv
Document Conventions .....	xv
Support Policy .....	xx
<b>CHAPTER 1 Choosing an Automated Installation Method .....</b>	<b>1</b>
Overview of Choosing an Automated Installation Method .....	2
Process for Choosing an Automated Installation Method .....	3
Fundamentals of Automated Installation .....	4
Choosing a Method Based on Clean Installations and Upgrades .....	7
Choosing a Method Based on Software Considerations .....	10
Choosing a Method Based on Operating System .....	11
Choosing a Method Based on Applications .....	12
Choosing a Method Based on Server Configuration .....	12
Choosing a Method Based on Network and Hardware Configurations .....	13
Choosing a Method Based on Network Topology .....	14
Choosing a Method Based on Hardware Inventory .....	15
Choosing a Method Based on Directory Services Considerations .....	16
Additional Resources .....	18
<b>CHAPTER 2 Designing Unattended Installations .....</b>	<b>19</b>
Overview of Unattended Installation .....	20
Unattended Installation Design Process .....	21
Unattended Installation Fundamentals .....	22
Evaluating Hardware and Software for Unattended Installations .....	24
Evaluating Hardware and Software Compatibility .....	26
Identifying Supplemental Device Drivers .....	27
Deciding Whether to Perform an Upgrade or a Clean Installation .....	28

Evaluating Possible Upgrade Paths .....	30
Evaluating Differences Between an Upgrade and a Clean Installation .....	32
Choosing a Distribution Method .....	33
Evaluating Distribution Methods .....	35
Using a Distribution Share to Perform an Unattended Installation .....	35
Using Media to Perform an Unattended Installation .....	37
Designing the Distribution Process .....	39
Designing a Distribution Share .....	39
Designing the Media Distribution Process .....	44
Designing Preinstallation Tasks for Unattended Installations .....	45
Creating a User State Migration Plan for Unattended Installations .....	47
Creating a Disk Configuration Plan for Unattended Installations .....	48
Planning for Dynamic Update .....	50
Identifying and Downloading Dynamic Update Files .....	51
Preparing Dynamic Update Files .....	52
Configuring Answer File and Winnt32.exe Settings for Dynamic Update .....	54
Designing Answer File and Setup Settings for Unattended Installations .....	55
Designing Automated Installation Tasks .....	58
Designing Automated Post-Installation Tasks .....	63
Identifying Automated Post-Installation Tasks .....	63
Choosing a Method for Automating Post-Installation Tasks .....	64
Configuring Cmdlines.txt to Perform Tasks .....	65
Configuring [GuiRunOnce] to Perform Tasks .....	66
Designing Setup Settings .....	68
Choosing Winnt.exe Parameters .....	68
Choosing Winnt32.exe Parameters .....	69
Creating Startup Media, Answer Files, and Distribution Shares .....	72
Creating Startup Media for Destination Computers .....	74
Choosing Startup Media .....	74
Creating Startup Media .....	76
Creating Answer Files .....	77
Creating an Answer File with Setup Manager .....	78
Creating an Answer File Manually .....	79
Creating Distribution Shares .....	80
Performing Unattended Installations .....	81

---

Performing a Clean Unattended Installation with an Operating System CD .....	83
Performing a Clean Unattended Installation with an MS-DOS Startup Disk .....	84
Performing a Clean Unattended Installation with a 32-bit Operating System .....	85
Performing an Unattended Upgrade Installation .....	86
Additional Resources .....	87
<b>CHAPTER 3 Designing Image-based Installations with Sysprep .....</b>	<b>91</b>
Overview of Image-based Installations .....	92
Image-based Installation Design Process .....	93
Image-based Installation Background .....	94
Identifying Inventory Requirements for Image-based Installations .....	97
Identifying Hardware That Impacts Image-based Installations .....	99
Identifying Software That Impacts Image-based Installations .....	103
Verifying Software and Hardware Compatibility .....	105
Defining Disk Images .....	106
Evaluating Operating System Differences .....	108
Evaluating Hardware Differences .....	108
Evaluating Software Differences .....	111
Evaluating Operating System and Software Settings .....	113
Designing the Image Delivery Process .....	114
Choosing a Disk-Imaging Program .....	116
Choosing an Image Distribution Method .....	117
Distributing Disk Images Across a Network .....	118
Distributing Disk Images by Using Media .....	119
Comparing Disk Image Distribution Methods .....	120
Designing Preinstallation Tasks for Image-based Installations .....	121
Creating a User State Migration Plan for Image-based Installations .....	123
Creating a Disk Configuration Plan for Image-based Installations .....	124
Designing Automated Setup Tasks .....	126
Automating Tasks Before Mini-Setup .....	128
Automating Tasks During Mini-Setup .....	133
Automating Tasks After Mini-Setup .....	138
Creating Disk Images .....	141
Building Master Installations .....	143
Preparing Master Installations by Running Sysprep .....	148
Identifying Cleanup, Configuration, and Auditing Tasks .....	148

Choosing Sysprep Settings .....	149
Creating Disk Images of Master Installations .....	152
Creating Startup Media for Destination Computers .....	153
Choosing Startup Media .....	154
Creating Startup Media .....	155
Deploying Disk Images .....	157
Additional Resources .....	158
<b>CHAPTER 4 Designing RIS Installations .....</b>	<b>161</b>
Overview of the RIS Deployment Process .....	162
Process for Deploying RIS .....	163
Planning RIS Installations .....	172
Identifying Client Requirements .....	174
Evaluating RIS Client Hardware .....	174
Determining RIS Client HAL Types .....	175
Evaluating Remote Boot Capabilities of RIS Clients .....	177
Auditing Existing Clients .....	180
Evaluating the RIS Client Prestaging Process .....	185
Evaluating Operating System Configurations .....	187
Evaluating RIS Server Requirements .....	190
Evaluating RIS Server Hardware Requirements .....	190
Assessing RIS Server Software Requirements .....	191
Assessing RIS Server Placement .....	192
Planning RIS Server Performance .....	195
Assessing Master Computer Requirements .....	198
Assess Existing Network Infrastructure .....	200
Evaluating Network Installation Points .....	202
Redirecting RIS Client Requests .....	203
Forwarding Client DHCP Requests through Routers .....	204
Planning RIS Network Security .....	204
Assessing the Security of the PXE Environment .....	205
Evaluating the NTLM Authentication Level .....	206
Assessing Security for Non-Prestaged Clients .....	206
Planning for Network Security Enhancement Using Prestaged Clients .....	207
Assessing Security Benefits of Restricting Client Installation Options .....	208
Assessing Security Benefits of Controlling the User Interaction Level .....	209
Evaluating Security for Operating System Images .....	210
Assessing RIS Server Authorization Security .....	211



---

Planning Security for RIS Administrative Tasks .....	212
Designing RIS-based Installations .....	215
Designing the RIS Installation Type .....	215
Design a Riprep-Based Installation .....	216
Riprep Image Design Background .....	216
Riprep Image Design Tasks .....	218
Riprep Image Design and User Profiles .....	223
Design a Risetup-Based Installation .....	223
Risetup Image Design Background .....	224
Risetup Image Design Tasks .....	225
Designing the RIS Deployment Mode .....	234
Interactive Installation Design Background .....	234
Interactive Installation Design Tasks .....	235
Fully-Automated Installation Design Background .....	238
Fully-Automated Installation Design Tasks .....	241
Designing the CIW Process .....	245
CIW Design Background .....	245
CIW Design Tasks .....	249
Designing the RIS Server Configuration .....	259
RIS Server Configuration Design Background .....	259
RIS Server Configuration Design Tasks .....	260
Designing the Active Directory Infrastructure .....	273
Designing a Test RIS Environment .....	276
Configuring and Deploying RIS .....	278
Creating a RIS Test Environment .....	279
Configuring Networking Support .....	280
Configuring Production Clients .....	281
Creating a Production RIS Server .....	282
Configuring a Master Installation .....	283
Installing the Master Computer Operating System .....	283
Configuring the Master Computer Operating System .....	284
Testing Riprep Images and User Profiles .....	285
Running the Riprep Wizard on the Master Computer .....	286
Configuring Answer File and Image Folder Permissions .....	286
Building a Master Distribution Share Installation .....	287
Configuring the RIS Server .....	287
Creating the CIW Configuration .....	289

Deploying an Operating System .....	290
Using a Network Boot .....	290
Using a RIS Boot Floppy Disk .....	291
Additional Resources .....	291
<b>CHAPTER 5 Migrating User State .....</b>	<b>295</b>
Overview of Migrating User State .....	296
User State Migration Process .....	297
Tools Used in the Migration Process .....	297
Choosing a User State Collection Method .....	300
Manual Migration .....	302
Scripted-Manual Migration .....	303
Centralized Automation .....	304
User-Driven Migration .....	306
Identifying Migration Content .....	307
Identifying User Data to Migrate .....	308
Identifying User Settings to Migrate .....	309
Identifying Key Settings for User Productivity .....	309
Evaluating Costs vs. Benefits of Migrating Settings .....	310
Creating a Detailed Migration Plan .....	311
Resolving Storage and Data Issues .....	312
Determining Storage Requirements .....	312
Reviewing Data Collection and Restoration Selections .....	313
Addressing File Relocation Issues .....	313
Identifying Security Concerns .....	314
Restoring Lost Access Control Lists (ACLs) .....	314
Managing Data Encryption During Migration .....	314
Securing User State During Migration .....	315
Translating and Relocating Registry Entries .....	315
Adapting Your Plan for Domain Migration .....	316
Scheduling Your Migration .....	317
Educating Users .....	318
Testing Your Migration Process .....	319
Performing Lab Tests .....	320
Performing a Pilot Test .....	320
Additional Resources .....	321
<b>GLOSSARY .....</b>	<b>323</b>
<b>INDEX.....</b>	<b>329</b>

## Acknowledgments

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

Documentation Manager: Pilar Ackerman

Writing Lead: Cheryl Jenkins

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

Editors: Nona Allison, Ann Becherer, Jim Becker, Bonnie Birger, Dale Callison, Anika Nelson, Tyler Parris, Susan Sarrafan, Scott Somohano, Dee Teodoro, Scott Turnbull, Tom Winn, Paula Younkin

Lab Management: Robert Thingwold, David Meyer

Project Managers: Clifton Hall, Paulette McKay, Neil Orit

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

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

Key Technical Reviewers: Linda Apsley, Jim Thatcher

Technical Reviewers: Michael Brinlee, Ryan Burkhardt, Nathan Cornillon, Mark Dietrich, Tony Donno, Bo Downey, Jim Edgar, Vinnie Flynt, Darrell Gorter, David Hennessey, Charlie Hough, Raj Jhanwar, Craig Marl, Scott McArthur, Wes Miller, Joseph Minckler, Madhulika Narayan, Calin Negreanu, Dennis Pollet, Andrew Ritz, Matt Seybold, Levi Stevens, Josh Vincent

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 *Automating and Customizing Installations* of the Microsoft® Windows® Server 2003 Deployment Kit. This book provides comprehensive information about planning, designing, and implementing automated installations in medium and large organizations. Options range from automated installations of a basic operating system to complex installations of a customized operating system and applications. The technologies and tools discussed in this book include: unattended installation, image-based installation with the System Preparation (Sysprep) tool, and Remote Installation Services (RIS). IT professionals can use the guidelines discussed in this book to create a functional specification that describes how to automate the installation of Windows Server 2003 and Windows XP Professional.

# 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 Support Tools.** A collection of tools included on the Windows Server 2003 operating system CD that you can use to diagnose and resolve computer and network problems.
- **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.


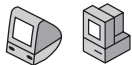




## Flowchart Symbols

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





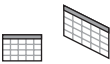
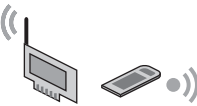













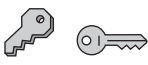






## Art Symbols

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

(continued)





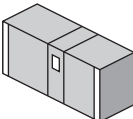
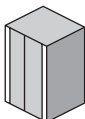
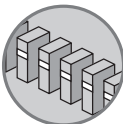




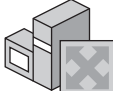

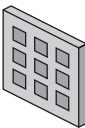
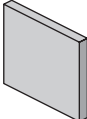
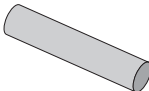


**(continued)**

	Portable digital assistant (PDA)		Document
	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

**(continued)**















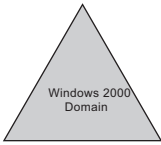
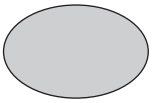
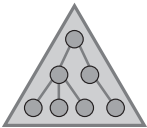


*(continued)*

	Modem bank		Automated library
	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






*(continued)*

(continued)

	Transceiver		Script
	Interface		Packets
	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
 <b>Tip</b>	Alerts you to supplementary information that is not essential to the completion of the task at hand.
 <b>Note</b>	Alerts you to supplementary information.
 <b>Important</b>	Alerts you to supplementary information that is essential to the completion of a task.
 <b>Caution</b>	Alerts you to possible data loss, breaches of security, or other more serious problems.
 <b>Warning</b>	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
<b>bold font</b>	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.
<code>Monospace font</code>	Code samples.
<b>Command</b>	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](mailto: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 2003 operating systems, please refer to the support information included with your product.

# Choosing an Automated Installation Method



Automated installations are faster, easier, less expensive, and more consistent than having users or IT professionals install the operating system manually. You can design and deploy automated installations by using one of three automated installation methods that are included with the Microsoft® Windows® Server 2003 family of operating systems. You can determine which method to use by evaluating your available resources, the existing or planned infrastructure, and the requirements of the configurations you plan to deploy.

**In This Chapter**

**Overview of Choosing an Automated Installation Method .....2**  
**Choosing a Method Based on Clean Installations and Upgrades .....7**  
**Choosing a Method Based on Software Considerations ..... 10**  
**Choosing a Method Based on Network and Hardware Configurations ..... 13**  
**Choosing a Method Based on Directory Services Considerations ..... 16**  
**Additional Resources..... 18**

**Related Information**

- For more information about designing unattended installations, see “Designing Unattended Installations” in this book.
- For more information about designing Remote Installation Services (RIS) installations, see “Designing RIS Installations” in this book.
- For more information about designing Sysprep-based installations, see “Designing Image-based Installations with Sysprep” in this book.

# Overview of Choosing an Automated Installation Method

There are three automated deployment methods you can use to perform automated operating system installations: Remote Installation Services (RIS), the System Preparation tool (Sysprep.exe), and the Unattended Setup tool (Winnt32.exe). You can use the automated installation tools included in the Windows Server 2003 family to automate and customize your corporate client or server operating system deployments. For organizations with many computers, automating installations is more efficient and cost-effective than using the interactive Setup program.

You need to design the client and server configurations that you want to deploy in your organization before you perform automated installations of the Windows Server 2003 or Microsoft® Windows® XP operating system. This includes designing the configuration of all networking, directory services, and security components. You need this client and server design information to customize your automated installation, as well as to help you decide which method is best to use. To choose which automated installation method is the best, you need to have access to complete information about the network topology, directory services, hardware inventory, and software inventory of your organization, and the time required to perform automated deployments within that infrastructure. You need to weigh all these considerations carefully and consider the benefits and limitations of each installation method, even if one of the considerations seems to point you definitively toward one of the methods. You might also determine that one method of automated installation is best for one set of circumstances in your organization, but that other installation circumstances in your organization are better suited for another method.

The scope of your deployment plan might also have an impact on your choice of deployment tools and methods. If you are planning a very large client-side remote installation on thousands of computers in one central location, consider the impact on network availability. If you are planning a number of smaller deployments in geographically remote locations, consider the methods you will need to use to distribute and install the operating systems and reference images.

When you have completed the tasks in this chapter you will be able to choose the automated installation method best suited for your organization. You can then begin designing your automated installation according to the guidelines in the appropriate design chapter for the method you have chosen.

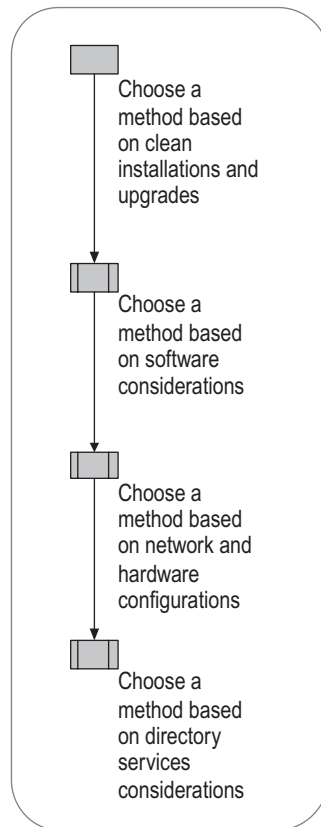
Considerations for choosing an automated installation method that are discussed in this chapter apply only to deployments and rollouts; they do not apply to ongoing operational tasks such as reinstallation after a hard disk failure or reinstallation caused by software or hardware failure.

## Process for Choosing an Automated Installation Method

To choose the best automated installation method for your situation, you need to systematically evaluate a variety of different aspects of your installation circumstances. These aspects include the logistics of the actual installation, the hardware and software involved in the installation, and the network and IT infrastructure of your organization. Use the hardware and software inventory and deployment plans of your organization as the source for this information. For more information about inventories, see “Planning for Deployment” in *Planning, Testing, and Piloting Deployment Projects* of this kit.

Figure 1.1 shows the process for choosing an automated installation method.

**Figure 1.1 Choosing Your Automated Installation Method**



The order of the tasks outlined in this chapter is designed to help you narrow your choices early in the process and fine-tune your decision toward the end of the process. Although your choice might appear clear early in the process, it is important that you carefully examine all of the factors that might affect your decision to be certain that you have not overlooked an important factor.

For a job aid to assist you in choosing an automated installation method, see “Choosing a Method for Automated Installation” (ACIOV\_01.xls) on the *Microsoft® Windows® Server 2003 Deployment Kit* companion CD (or see “Choosing a Method for Automated Installation” on the Web at <http://www.microsoft.com/reskit>). Answering the questions listed in the job aid, as you read the information in this chapter, can help you determine the best automated installation method for your environment. This job aid is designed to be used online.

---

## Fundamentals of Automated Installation

You can automate and customize installations by using answer files, scripts, and batch files that configure the operating system and applications automatically by using several installation tools provided with the Windows Server 2003 family.

### Basic Concepts of Automated and Customized Installations

An *automated installation* runs with minimal or no user interaction. This provides a faster, more consistent, and trouble-free installation. The automated installation tools use two basic methods to accomplish an automated installation:

- An *image-based installation* is a method of copying, or cloning, a preconfigured operating system and software applications from a master computer onto destination clients and servers. For the purposes of this chapter, the term *image-based installation* refers to installations using Sysprep or the Remote Installation Preparation Wizard (Riprep.exe) installation tool.
- An *answer file-based installation* uses a text file that contains setup instructions. These instructions include:
  - Answers to the questions that Windows Setup normally presents during an installation.
  - Instructions for configuring operating system settings.
  - Instructions for installing applications without user intervention.

For the purposes of this chapter, the term *answer file-based* installations refers to installations using the Unattend and Remote Installation Services Setup (Risetup.exe) installation tools.



A *custom installation* is an operating system installation that is modified to support specific hardware and software configurations and meets specific organizational and user needs. You can customize an automated installation by using the configuration and setting design information that you have determined for your Windows Server 2003 family and Windows XP deployment, including applications, additional language support, service packs, and device drivers. You customize an automated installation by:

- Modifying the answer file to provide the Setup program with specific answers and instructions.
- Adding custom files, applications, and programs to the distribution folder.
- Modifying the configuration of the master computer.

### Windows Server 2003 Automated Installation Tools

Three automated installation tools are included with the Windows Server 2003 family. Each is described briefly in the following sections.



#### Note

You can start a destination computer by using a Windows Preinstallation Environment (Windows PE) CD, and then using the **diskpart** command to partition a disk and the **format** command to format a disk. WinPE is a bootable operating system that provides limited operating system functionality for performing preinstallation tasks. Windows PE is only available if you have purchased Enterprise Agreement 6.0, Enterprise Subscription Agreement 6.0, or Select License 6.0 with Software Assurance (SA). For more information about Windows PE and Windows PE licensing plans, see the Windows Preinstallation Environment link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

### Remote Installation Services

With RIS, you can design a destination computer-initiated automated installation scenario to deploy clean, preconfigured, file system image-based or script-based installations on multiple client computers from remote master server computers over a network connection. Using RIS, you can create and store reference images on a server; the destination computers initiate the installation process. RIS is the only method you can use to install an operating system without the need for an administrator to physically visit each computer to initiate the installation.

You can use two components of RIS to perform remote installations in different ways: Remote Installation Services Setup (Risetup.exe) and Remote Installation Preparation Wizard (Riprep.exe). The following summarizes the differences:

- **Risetup.exe.** You use this component to set up the RIS server and create a distribution folder for the operating system and software files for the installation.
- **Riprep.exe.** You can use Riprep.exe to create a customized image of an operating system such as Microsoft® Windows® XP Professional. Use Riprep to prepare an image from an existing operating system installation on a master computer and replicate that image to an available RIS server on your network. The image can include the operating system with default parameters applied, or the operating system with a preconfigured desktop, locally installed applications, and drivers.

RIS is a service that requires a dedicated server. You must also configure your network and domain to use RIS. For more information see “Designing RIS Installations” in this book.

### **Sysprep**

You can use the System Preparation tool (Sysprep) to prepare a master computer for disk imaging after performing the initial setup steps on that computer. Sysprep assigns a unique security identifier (SID) to each destination computer the first time the computer is rebooted. Using Sysprep is the fastest way to set up a computer. Applying a Sysprep disk image to a destination computer takes just a few minutes.

With a third-party disk-imaging tool, you can copy the contents of the hard disk (a Sysprep disk image) of a master computer onto removable media. You can use this disk image to quickly install exact copies of the master computer onto the hard disk of destination computers in your organization.

Sysprep (Sysprep.exe) is in the Deploy.cab file in the \Support\Tools folder on the Windows XP Professional or Windows Server 2003 operating system CD. For more information see “Designing Image-based Installations with Sysprep” in this book.

### **Unattended Installation**

Unattended installation (Unattended Setup) uses an answer file to automate the answers to the questions Windows Setup normally presents to the user during the installation. An answer file can also contain instructions for configuring operating system settings and installing applications without user intervention. You can, by means of a distribution share or media, distribute the answer file and any device drivers and other files that are required to customize the installation. Unattended installations take longer to perform because all of the files are copied to the destination computer.

Unattended installation consists of two command-line tools:

- **Winnt32.exe**, used when starting your installation from the Microsoft® Windows® 95, Windows® 98, Windows NT®, or Windows® 2000 operating systems.
- **Winnt.exe**, used when starting your installation from the Microsoft® Windows® 3.1, Microsoft® Windows® for Workgroups, and MS-DOS® operating systems.

These tools are in the \i386 folder on the Windows XP Professional or Windows Server 2003 operating system CD. For more information, see “Designing Unattended Installations” in this book.

---

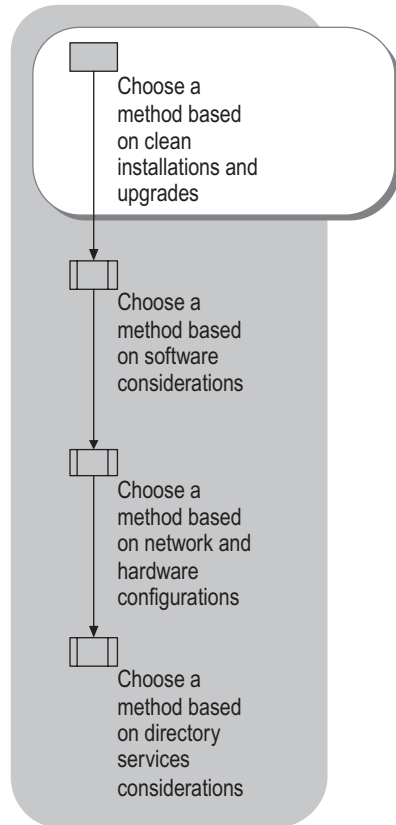
## Choosing a Method Based on Clean Installations and Upgrades

The decision to perform either clean operating system installations or upgrades is important when determining the best automated installation method to use. When moving to a new operating system, most organizations choose to perform clean installations. This helps them to maintain uniformity and, for client computers, to reset the corporate-installed base. If, however, you have older line-of-business applications or peripherals that you plan to continue using in your organization after moving to the new operating system, you might need to perform an upgrade to retain the ability to use those applications and device drivers.

If you are deploying clean installations of Windows XP Professional or Windows Server 2003, you can use any of the Windows Server 2003 automated installation methods. Before you perform a clean installation or an upgrade, test the installation of your older software and device drivers to be sure they work. For more information about performing upgrades, clean installations, and upgrade paths, see “Planning for Deployment” in *Planning, Testing, and Piloting Deployment Projects* of this kit.

Figure 1.2 illustrates the place of this step in the process of choosing an automated installation method.

**Figure 1.2 Choosing a Method Based on Clean Installations and Upgrades**



## Installation Tools for Upgrading the Operating System

You cannot use RIS or Sysprep to upgrade an operating system. The only automated installation method you can use to perform upgrades is unattended installation using Winnt32.exe. You cannot use Winnt.exe to perform an upgrade.

Because some registry settings and system files are retained when you perform an upgrade, you need to thoroughly test your upgrade scenarios in your test lab before rolling out the installation to the production environment. Testing the upgrade can help avoid unexpected loss of data or configurations. For more information about designing an unattended installation, see “Designing Unattended Installations” in this book.

## Installation Tools for Performing Clean Installations

You can use any of the Windows Server 2003 automated installation tools to perform clean installations of the operating system. If you are deploying clients and you want to retain user settings and data before using an automated installation method to deploy clean installations, consider using the User State Migration Tool (USMT). The guidelines outlined in the remainder of this chapter help you determine which of the Windows Server 2003 automated installation tools is best for a clean installation in your organization.



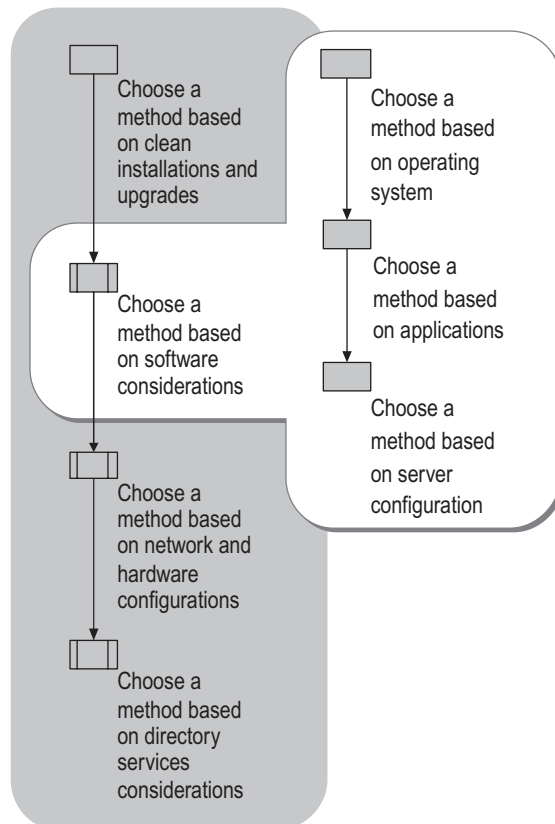
### Note

The USMT tool is included on the Windows Server 2003 operating system CD in the \ValueAdd\Msft\USMT folder.

# Choosing a Method Based on Software Considerations

Software considerations that affect your automated installation method include whether you plan to deploy server or client operating systems, what types of applications you plan to deploy along with the operating system, and the configuration of servers you plan to deploy. Figure 1.3 illustrates the place of this step in the process of choosing an automated installation method.

**Figure 1.3** Choosing a Method Based on Software Considerations



## Choosing a Method Based on Operating System

An important consideration when choosing your automated installation method is whether you are planning to deploy client or server operating systems. Answer file-based methods provide an opportunity to do the type of fine-tuned configuration necessary for deploying servers, and image-based methods are ideal for quickly deploying a common desktop environment to many client computers.

### Installing on Client Computers

An image-based automated installation method is ideal for quickly deploying standard configurations to client computers. The device drivers for most Plug and Play devices for standard desktop and portable computers are included in Windows XP Professional, so no additional configuration is needed, even if these devices vary in your organization.

However, inventory your hardware to be certain that your device drivers are included in the installation. If you have a large number of desktop or portable computers that have a variety of specialized device drivers or drivers that are not included with Windows XP, an answer file-based method provides a way to reconfigure the installation with the appropriate drivers.

**Note**

If you are using RIS to add a large number of client computers to an existing environment, include capacity planning in your deployment design to ensure an adequate level of service availability during the installation process.

### Installing on Servers

Different considerations apply to installations on individual servers that have varying roles throughout the organization and installations on members of a server farm. Consequently, you might choose different installation methods for individual servers and server farms.

#### Installing on individual servers

Because installing a server operating system often involves customizing configurations, especially when deploying several different roles in a single installation, an answer file-based automated installation method is ideal.

#### Installing on server farms

Server farms, especially load-balanced server farms, often require identical configuration of the servers in the farm. Using Sysprep to set up the servers quickly with the same configuration can be the most efficient choice in this situation. If you are using Windows Network Load Balancing (NLB) as your load-balancing solution, however, you must script the installation and configuration of NLB after installing the operating system by using Sysprep.

## Choosing a Method Based on Applications

If you are planning to install applications together with the operating system, considerations that might affect your choice of automated installation methods include the compatibility of the application with the installation method.

### Testing Application Installation Compatibility for Image-Based Installations

If you are planning an image-based installation and plan to install applications with the operating system, you need to thoroughly test the installation. Although most applications should copy correctly, some configurations, settings, or other aspects of the application might cause an application to behave unexpectedly after an image-based installation. If your applications do not install properly on an image, you can install by using Unattended Setup instead.

---

## Choosing a Method Based on Server Configuration

If you are installing a server operating system, your plans for configuring the operating system affect the installation method you choose.

### Planning for Certificate Services

You can use an answer file-based automated installation method to install and configure Certificate Services as part of the installation. However, when you use an image-based installation method, you must install and configure Certificate Services after the installation is complete.

### Planning for the Cluster Service

You can use an answer file-based automated installation method to install and configure the Cluster service as part of the installation. However, when you use an image-based installation method, you must install and configure the Cluster service after the installation is complete.

### Planning for Domain Controllers

As part of an answer file-based automated installation, you can include a script that starts the Active Directory Installation Wizard (Dcpromo.exe) to configure a server as a domain controller. However, when you use an image-based installation method, you must configure servers as domain controllers after the installation is complete.

### Planning for Internet Information Services

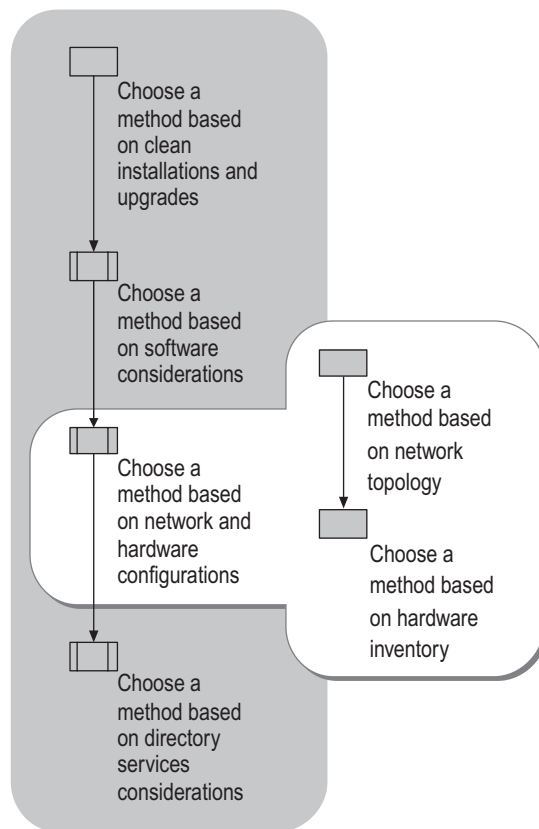
The configuration settings for Internet Information Services (IIS) are built into the answer files used with Unattend and Risetup; therefore these methods are the most efficient way to deploy IIS servers. However, image-based installation of an IIS server is fully supported.



# Choosing a Method Based on Network and Hardware Configurations

There are several network topology and hardware considerations that affect your automated installation. Figure 1.4 illustrates the place of this step in the process of choosing an automated installation method.

**Figure 1.4** Choosing a Method Based on Network and Hardware Configurations



## Choosing a Method Based on Network Topology

Network bandwidth and existing network protocols are important factors in deciding which automated installation method to use. For example, if you do not have a high-bandwidth connection to a network server, a method that uses media such as a CD-ROM or DVD for the installation is usually more appropriate than using RIS for automated installations.

### Examining Network Connectivity

To use RIS or to perform an installation by using Sysprep or Unattend from a share, you need to have reliable, high-bandwidth network connections in place. RIS requires that a TCP/IP network be in place. This is not a requirement for Unattend and Sysprep.

If the destination computers for your automated installation are connected to the network by low-bandwidth connections, such as when you have clients located in remote locations, an automated installation method that you install from a disk, such as Sysprep or Unattend, is better than a RIS-based installation. RIS requires that a robust network be in place. Installations performed with Sysprep or Unattend take place locally on the computer. Nothing needs to travel across the network.



#### Note

To use RIS for automated installation, you need a network card that supports Pre-Boot eXecution Environment (PXE) technology. Wireless network cards and many token ring network cards do not support PXE. For more information, see “Choosing a Method Based on Hardware Inventory” later in this chapter.

### Examining IP Address Allocation

After an image created with Sysprep or Riprep is copied onto a destination computer, you must configure static IP address settings. When a disk image is copied onto a destination computer, all of the network adapters on the destination computer are initialized to the default settings, which include dynamic allocation of IP addresses. For this reason, an answer file-based installation method might be more convenient to use when you need to configure static IP addresses. For more information about how Sysprep affects network settings, see article Q271369, “Statically-Entered TCP/IP Settings Are Not Present After Sysprep” 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>.

RIS requires the presence of an active Dynamic Host Configuration Protocol (DHCP) server on the same network as the client computers. The remote boot-enabled client computers receive an IP address from the DHCP server prior to contacting the RIS server. Routers in a multi-subnet network are configured to forward the DHCP packets between the client and the RIS server. In addition, on routed networks, DHCP packets must be relayed to the RIS server as well as the DHCP server. For more information, see “Designing RIS Installations” in this book.

## Choosing a Method Based on Hardware Inventory

When choosing your automated installation method, a number of considerations about the hardware of both destination and master computers might affect your choice of methods. These include both compatibility and configuration considerations. In general, if you are deploying to a homogeneous hardware base, an image-based automated deployment method is optimal. However, if you are deploying to a heterogeneous hardware base, such as older hardware with varying drivers that are not included with the operating system that you are deploying, an answer file-based automated deployment method is optimal.

### Examining HAL Compatibility

You can only perform an image-based installation (using Sysprep or Riprep) if the hardware abstraction layer (HAL) on the disk image is compatible with the hardware on the destination computer. For example, if the master computer on which you run Sysprep or Riprep has an Advanced Configuration and Power Interface (ACPI) HAL, then the destination computers you designate to receive operating system images generated from that master computer must also have ACPI HALs. In some cases, you can upgrade the HAL that is on a disk image to suit the HAL requirements of a destination computer, but you must be certain that the HAL is compatible for this type of upgrade. If the HALs of the master computer and the destination computers are not compatible, an answer file-based installation method might be more convenient.

### Evaluating Support for PXE

To initiate a RIS-based operating system installation, a RIS client must first perform a remote network boot by connecting to a RIS server over the network. To make a remote boot possible, both the network adapter and ROM BIOS of the destination computer need to support PXE.

It is possible to emulate PXE support by using a Peripheral Component Interconnect (PCI)-based network adapter that boots from a RIS boot floppy. The RIS boot floppy is a startup disk that simulates the PXE startup process for computers that lack a remote boot-enabled BIOS. The Remote Boot Floppy Generator tool (Rbfg.exe), which is a part of RIS and is located on the RIS server, allows you to generate RIS boot floppy disks for use with RIS clients that are not PXE-enabled. Rbfg.exe supports a limited number of PCI cards. It is not possible to add support for a card that is not supported by the disk. You can obtain a list of supported network cards by clicking the **Adapter List** button in the rbfg.exe application.

If the network adapter and ROM BIOS of the destination computer do not support PXE, either Unattended Setup or Sysprep might be a more convenient choice for automated installation.

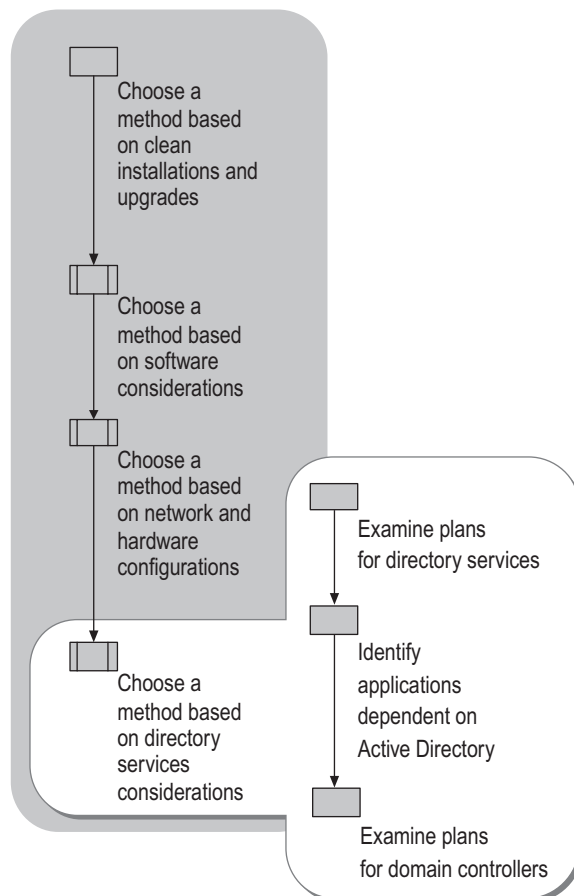
### Evaluating Mass Storage Controllers

Examine the mass storage controllers in your organization. If you have mass storage controllers that are not listed in any device information (.inf) file, such as Machine.inf, Scsi.inf, Pnp SCSI.inf, or Mshdc.inf, you need to specially configure the Mini-Setup stage of an image-based installation. In this case, the overhead involved might indicate that using Unattended Setup or Risetup is a better choice.

# Choosing a Method Based on Directory Services Considerations

When choosing your automated installation method, you need to consider the directory service your organization has in place. Figure 1.5 illustrates the place of this step in the process of choosing an automated installation method.

**Figure 1.5** Choosing a Method Based on Directory Services Considerations



### **Examining Plans for Directory Services**

If you plan to use RIS for automated installations, you must be using the Active Directory® directory service. RIS relies on Active Directory for security and computer account placement. In addition, RIS uses Active Directory to identify RIS clients and RIS servers.

### **Identifying Applications That Are Dependent on Active Directory**

Identify any applications that you plan to include with the automated installation that are dependent on Active Directory, such as client applications that access human resources or proprietary data. These applications cannot be installed and configured on a Sysprep image. You must install and configure these applications after the disk image is copied onto the destination computer and the computer is restarted. In this case, an Unattended Setup installation might be a better choice because Active Directory-dependent applications can be included with the rest of the installation.

### **Examining Plans for Domain Controllers**

Special considerations apply if you intend to create domain controllers by using an automated installation method. You cannot configure a Sysprep master computer as a domain controller. You need to first configure a master computer as a stand-alone server, and then install Active Directory by using the Active Directory Installation Wizard (Dcpromo.exe) after the disk image is copied onto a destination computer. However, you can script Dcpromo.exe with an answer file, and you can use the GuiRunOnce entry in your answer file to automatically start it at the end of an Unattended Setup. This is, therefore, a more efficient choice for installing preconfigured domain controllers.

# Additional Resources

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

## Related Information

- “Designing Unattended Installations” in this book.
- “Designing RIS Installations” in this book.
- “Designing Image-based Installations with Sysprep” in this book.
- The Windows Catalog link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources> for information about hardware and software that is compatible with the Windows Server 2003 family and Windows XP.

## Related Tools

- Deploy.cab

The Deploy.cab file contains the Sysprep tool and the Setup Manager tool, along with other related automated installation tools. The Deploy.cab file also contains the Microsoft Windows Preinstallation Reference file (Ref.chm), which has information about answer file sections, keys, and values; and the *Microsoft Windows Corporate Deployment Tools User's Guide*, which has detailed information about performing an automated installation. The Deploy.cab file is in the \Support\Tools folder on the Windows XP Professional and Windows Server 2003 operating system CDs. You can use Windows Explorer or run Extract.exe to extract and view the Ref.chm file.

## 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.

- “Planning for unattended Setup” in Help and Support Center for Windows Server 2003.
- “Remote Installation Services” in Help and Support Center for more information about installing and managing RIS for Windows Server 2003.

## Related Job Aids

“Choosing an Automated Installation Method” (ACIOV\_01.xls) (or see “Choosing an Automated Installation Method” on the Web at <http://www.microsoft.com/reskit>).

# Designing Unattended Installations

2

Unattended installation is the most flexible and versatile automated method of deploying the Microsoft® Windows® XP Professional operating system and the Microsoft® Windows® Server 2003 operating system. You can automate both clean installations and upgrades, and you can automate the installation and configuration of a wide range of system settings and system components without running batch files or scripts. Unattended installations also speed up the deployment process, minimize user involvement during installation, and ensure consistency throughout your organization, which lowers support costs.

## In This Chapter

<b>Overview of Unattended Installation .....</b>	<b>20</b>
<b>Evaluating Hardware and Software for Unattended Installations .....</b>	<b>24</b>
<b>Deciding Whether to Perform an Upgrade or a Clean Installation .....</b>	<b>28</b>
<b>Choosing a Distribution Method .....</b>	<b>33</b>
<b>Designing Preinstallation Tasks for Unattended Installations .....</b>	<b>45</b>
<b>Designing Answer File and Setup Settings for Unattended Installations .....</b>	<b>55</b>
<b>Creating Startup Media, Answer Files, and Distribution Shares.....</b>	<b>72</b>
<b>Performing Unattended Installations.....</b>	<b>81</b>
<b>Additional Resources.....</b>	<b>87</b>

## Related Information

- For more information about automated installations, see “Choosing an Automated Installation Method” in this book.
- For more information about image-based installations, see “Designing Image-based Installations with Sysprep” in this book.
- For more information about Remote Installation Services (RIS), see “Designing RIS Installations” in this book.

# Overview of Unattended Installation

Unattended installations are commonly used to perform bulk installations with minimal user intervention. Unattended installations are particularly useful if you are:

- Upgrading a Windows operating system to Windows XP Professional or Microsoft® Windows Server 2003, Standard Edition; Microsoft® Windows Server 2003, Web Edition; or Microsoft® Windows Server 2003, Enterprise Edition operating systems.
- Performing automated installations on computers that have heterogeneous hardware configurations.
- Performing automated installations on specific types of servers, such as domain controllers, remote access servers, and servers that run Certificate Services or the Cluster service.
- Configuring a wide range of operating system settings during an automated installation without using batch files and scripts.

In addition to these deployment solutions, unattended installation is a useful method of creating master installations for image-based and RIS installations.

As a deployment solution, unattended installation requires substantial up-front planning and design. This chapter is designed to help IT professionals in medium and large organizations plan and design an unattended installation. It is assumed that you have already read “Choosing an Automated Installation Method” in this book. It is also assumed that you have designed the client and server configurations that you want to deploy in your organization. This includes designing the configuration of all networking, directory services, and security components. You will use this client and server design information throughout this chapter to customize your unattended installation. When you finish the planning and design work described in this chapter, you will be ready to perform an unattended installation.

**Note**

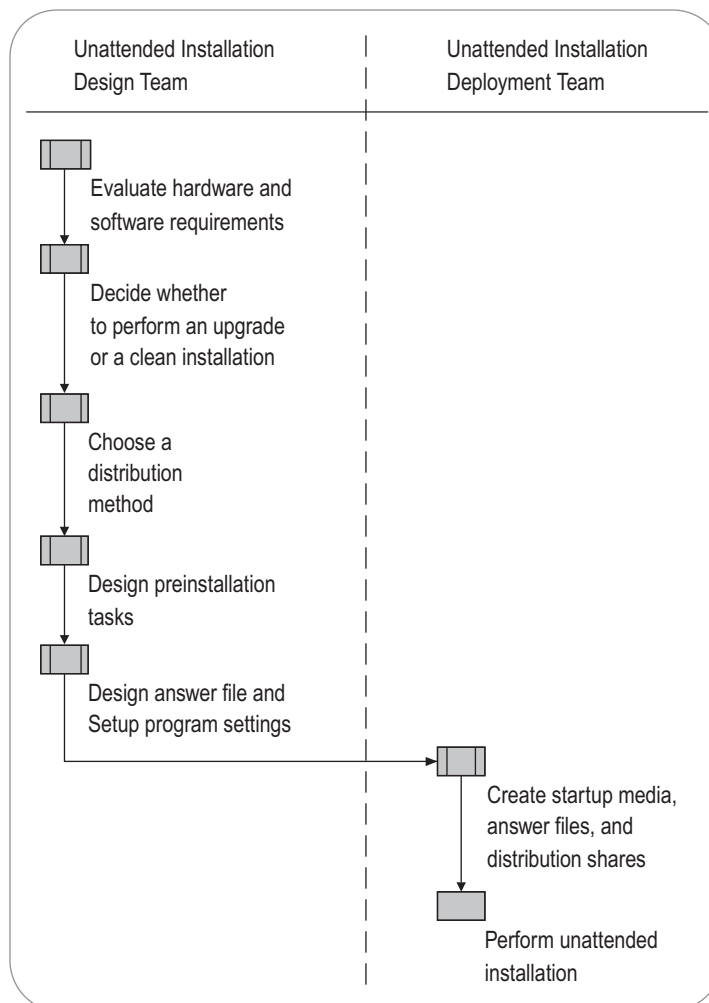
You cannot perform an unattended installation of Windows Server 2003, Datacenter Edition.



## Unattended Installation Design Process

Planning and designing an unattended installation involves a design team and a deployment team. The design team is responsible for assessing your current environment, deciding whether to upgrade or to perform clean installations, and designing the overall deployment process, including the distribution mechanism, preinstallation tasks, and automated installation and post-installation tasks. The deployment team is responsible for implementing all design decisions, including creating answer files, distribution shares, and startup media. The steps in this decision-making process are shown in Figure 2.1.

**Figure 2.1 Designing Unattended Installations**



## Unattended Installation Fundamentals

To perform an unattended installation, you first create an *answer file* — a text file that contains answers to the questions that Windows Setup normally prompts you for during an installation. An answer file also can contain instructions for configuring operating system settings and installing applications without user intervention. After you configure your answer file, you typically create a *distribution share* — a folder that contains the Windows XP Professional or Windows Server 2003 installation files, as well as any device drivers or other files that are required to customize the installation. A distribution share uses a hierarchical folder structure that is similar to the one used on computers running Windows Server 2003 or Windows XP Professional, and is typically stored on a server to which your destination computers can connect and retrieve copies of the files during an unattended installation.



### Note

You do not need to use a distribution share to perform an unattended installation; you can use an operating system CD instead of a distribution share.

After you have created an answer file and a distribution share, you are ready to start an unattended installation on a destination computer. To do this, you must run one of two Windows Setup programs: Winnt.exe or Winnt32.exe. Winnt.exe runs on 16-bit operating systems, including Microsoft® MS-DOS®, Microsoft® Windows 3.1, and Microsoft® Windows® for Workgroups operating systems. Winnt32.exe is used on 32-bit operating systems, including Microsoft® Windows® 95, Microsoft® Windows® 98, Microsoft® Windows® Millennium Edition, Microsoft® Windows NT®, Microsoft® Windows® 2000, Windows XP Professional, and Windows Server 2003 operating systems. Usually, you start the destination computer with a floppy disk that has been formatted as an MS-DOS startup disk, an operating system CD, or the existing operating system that is on the computer's hard disk. Depending on the operating system that is running on the destination computer, you then run either Winnt.exe or Winnt32.exe.

When you run Winnt.exe or Winnt32.exe to perform an unattended installation, you specify various command-line parameters. For example, you specify the name of the answer file you want Setup to use, and the location of the distribution share that contains the installation files. You also can specify various options, including whether to use Dynamic Update, whether to install Emergency Management Services, or whether to install the Recovery Console. Setup then runs and carries out all of the instructions specified in the answer file.

## New in Windows Server 2003 and Windows XP Professional

Several answer file headings and entries are new for Windows Server 2003 and Windows XP Professional. In addition, some headings and entries have been modified, and some headings and entries found in earlier versions of Windows no longer apply to Windows Server 2003 and Windows XP Professional. For more information about answer file changes, see “Changes in Answer Files” in *Microsoft® Windows Corporate Deployment Tools User’s Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.

## Unattended Installation Terms and Definitions

The following key terms are associated with unattended installations.

**Setup Manager** A program that creates answer files and distribution shares for unattended installations. Setup Manager (Setupmgr.exe) is included in the Deploy.cab file in the Support folder on the Windows XP Professional and Windows Server 2003 operating system CDs.

**Unattend.txt** The default name of the answer file that you use to automate Windows Setup during an unattended installation. Unattend.txt contains headings and parameters that instruct Setup to perform various configuration tasks.

**Winnt.sif** The name you give Unattend.txt when you perform an unattended installation by using the operating system CD instead of a distribution share.

**Cmdlines.txt** A configurable text file that you use to customize an unattended installation. Cmdlines.txt contains a list of commands that run synchronously after Setup finishes, but before a computer restarts. Cmdlines.txt can exist on the destination computer’s hard disk or on a floppy disk, and must be specified in the [Unattended] section of Unattend.txt or Winnt.sif.

**[GUIRunOnce]** A section in your answer file that is used to customize an unattended installation. The [GUIRunOnce] section contains a list of commands that run synchronously after a destination computer is started for the first time and a user logs on.

**Mini-Setup** A wizard that is a subset of Windows Setup. Mini-Setup provides prompts for user-specific information, configures operating system settings, and detects new hardware. You can automate Mini-Setup by using a Sysprep.inf answer file.

**File-copy mode** The first of the three stages of Setup, where the Windows program files and any additional files specified are copied to the computer's hard disk.

**Text Mode** The second of the three stages of Setup, during which Setup determines the basic hardware of the computer (CPU, motherboard, hard disk controllers, file systems, and memory), installs the base operating system necessary to continue, and creates specified folders.

**GUI mode** The third of the three stages of Setup, during which Setup configures the computer's hardware and network settings, prompts you to provide an Administrator password, and allows you to customize the installation.

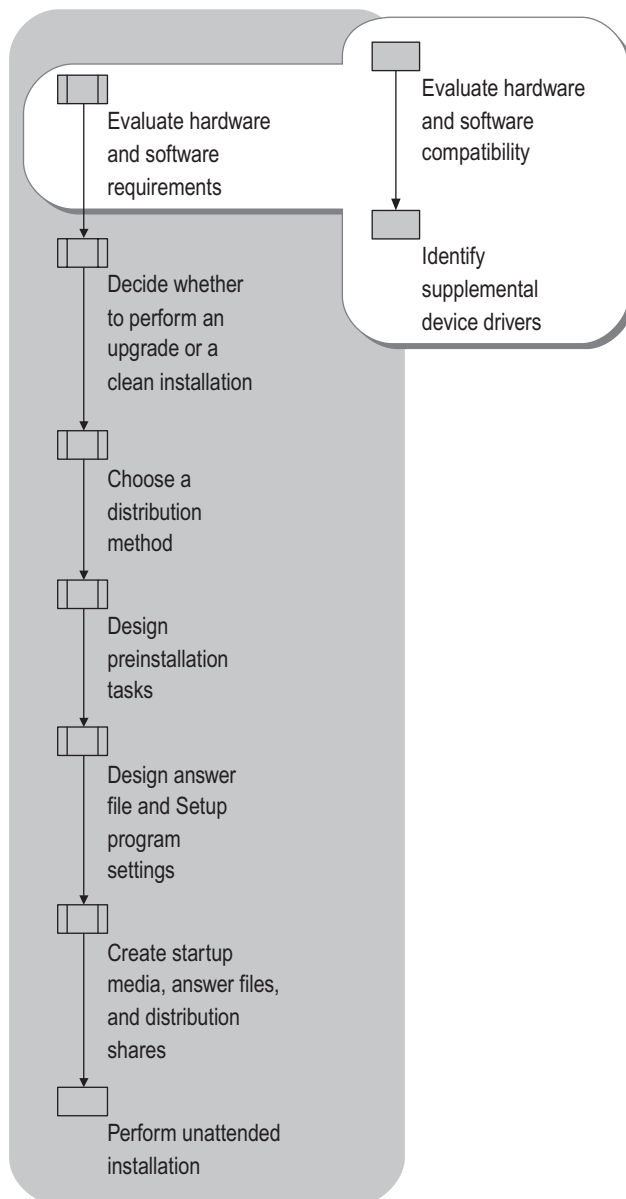
---

## Evaluating Hardware and Software for Unattended Installations

Before you start designing an unattended installation, you must determine whether the hardware and software on your destination computers is compatible with the operating system you are deploying, and whether you have the appropriate device drivers for an unattended installation. You can use your hardware and software inventory to identify the hardware and software that is installed on your destination computers. For more information about creating a hardware or software inventory, see "Planning for Deployment" in *Planning, Testing, and Piloting Deployment Projects* of this kit.

Figure 2.2 shows the steps you need to follow to evaluate hardware and software for unattended installations.

**Figure 2.2 Evaluating Hardware and Software**



## Evaluating Hardware and Software Compatibility

You must evaluate hardware and software compatibility before you perform an unattended installation because incompatibilities can cause an unattended installation to fail. For example, if Setup attempts to install a device or an application that is incompatible during an unattended installation, Setup cannot display a warning dialog box or prompt a technician for alternative installation instructions. Instead, Setup simply stops running, and the installation fails. Therefore, you must replace or upgrade incompatible hardware and software before you perform an unattended installation.

### Evaluating Hardware Compatibility

You can use several resources and tools to verify hardware compatibility.

#### **Windows Catalog**

The Windows Catalog contains a list of software and hardware products that are designed for, or are compatible with, Windows XP Professional and Windows Server 2003. You can search the catalog by manufacturer, product type, product name, or model. If you do not see a product in the Windows Catalog, it does not mean the product will not work with Windows XP or Windows Server 2003 — check with the product's manufacturer to determine whether the product works with these versions of Windows. For more information, see the Windows Catalog link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

#### **Windows Upgrade Advisor and Windows XP Upgrade Advisor**

Windows Upgrade Advisor and Windows XP Upgrade Advisor are tools that check your system hardware and software to see whether they are ready to be upgraded to Windows XP Professional or Windows Server 2003. Although the tools assume you are upgrading to Windows XP Professional or Windows Server 2003, you also can use them to identify software and hardware that are not compatible during a clean installation of Windows XP Professional or Windows Server 2003. To download either of the tools, see the Windows Upgrade Advisor link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>. You also can run either tool by using the **/checkupgradeonly** parameter with Winnt32.exe. Winnt32.exe is included in the i386 folder on any Windows XP Professional or Windows Server 2003 operating system CD.

## Evaluating Application Compatibility

In addition to Windows Catalog and Windows Upgrade Advisor, you can use the Application Compatibility Toolkit to verify software compatibility. The Application Compatibility Toolkit contains documents and tools to help you diagnose and resolve application compatibility issues with Windows XP Professional and Windows Server 2003. For more information about application compatibility, see “Planning and Testing for Application Deployment” in *Planning, Testing, and Piloting Deployment Projects* of this kit. For more information about the Application Compatibility Toolkit, see article Q294895, “Description of the Application Compatibility Toolkit 2.0 for Windows XP,” 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>.

---

## Identifying Supplemental Device Drivers

Most device drivers are provided on the Windows XP Professional and Windows Server 2003 operating system CDs. However, some devices require special device drivers, which you must obtain from the hardware vendor. Some devices that require special drivers include:

- Plug and Play devices for which there are no device drivers on the operating system CD. Sound cards and video adapters on portable computers are common examples.
- Mass storage controllers, particularly small computer system interface (SCSI) controllers and redundant array of independent disks (RAID) controllers.
- Hardware abstraction layers (HALs) created by a third party.
- Legacy (non-Plug and Play) devices for which there are no device drivers on the operating system CD.

When you obtain device drivers from a third party, make sure that Microsoft has digitally signed the device drivers. Signing ensures that the device driver has undergone a certain level of testing, and that the device driver cannot be altered or overwritten by another program’s installation process. Device driver files can include: system (.sys) files, dynamic-link library (.dll) files, information (.inf) files, and text setup (Txtsetup.oem and Txtsetup.sif) files.

In addition to making sure that you have the appropriate device drivers for your hardware, you need to make sure that the device drivers are available to Setup during the unattended installation process. If they are not, Setup might stop running and the unattended installation might fail. To make sure device drivers are available to Setup, you need to save the device drivers in a distribution share so they are copied to the destination computer during an unattended installation, or you need to save the device drivers on the destination computer's hard disk before you initiate the installation.

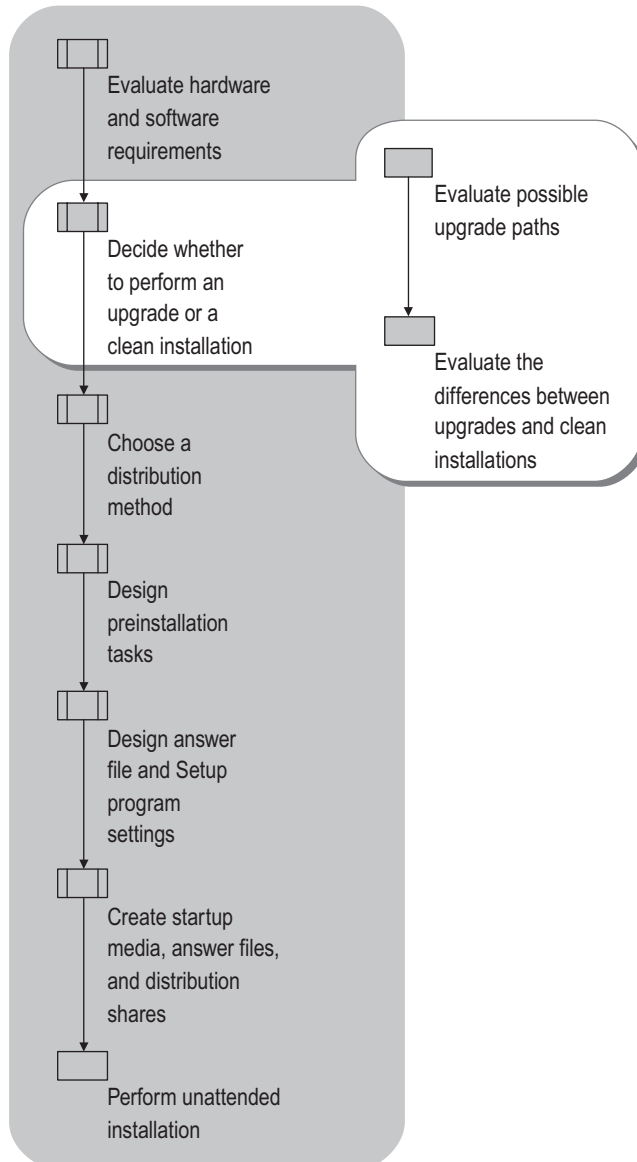
For a worksheet to help you record information about supplemental device drivers, see "Unattended Installation Worksheet" (ACIUI\_1.doc) on the *Microsoft® Windows® Server 2003 Deployment Kit* companion CD (or see "Unattended Installation Worksheet" on the Web at <http://www.microsoft.com/reskit>). For more information about device-driver signing and how Windows selects device drivers, see "Using Signed Drivers" in *Microsoft Windows Corporate Deployment Tools User's Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.

---

## Deciding Whether to Perform an Upgrade or a Clean Installation

Unlike other automated installation methods, such as image-based and RIS installations, an unattended installation can be configured to perform a clean installation or an upgrade of an existing operating system. To determine which installation method is more appropriate, you need to evaluate possible upgrade paths, and then evaluate the advantages and disadvantages of upgrades and clean installations. If you determine that upgrading is appropriate, you then identify upgrade issues that you need to address during the planning and design phase of an unattended installation. Figure 2.3 shows the steps you need to follow to determine whether to perform an upgrade or a clean installation.



**Figure 2.3 Determining Whether to Perform an Upgrade or a Clean Installation**

## Evaluating Possible Upgrade Paths

If the computer on which you want to install Windows Server 2003 or Windows XP Professional is running Windows 95, Windows 3.1, or Microsoft® Windows NT® Server version 3.51, you need to perform a clean installation. In addition, you need to choose clean installation if you are using Windows 98, Windows Millennium Edition, Microsoft® Windows NT® Workstation version 4.0, Microsoft® Windows® 2000 Professional, or Windows XP Professional operating systems and you want to install Windows Server 2003. In most other cases, you can choose to upgrade. Table 2.1 shows the possible upgrade paths for Windows XP Professional and Windows Server 2003.

**Table 2.1 Upgrade Paths for Windows XP Professional and Windows Server 2003**

Existing Operating System	Upgrade to Windows XP Professional	Upgrade to Windows Server 2003, Standard Edition	Upgrade to Windows Server 2003, Enterprise Edition	Upgrade to Windows Server 2003, Web Edition
Windows NT Server 3.51				
Microsoft® Windows NT® Server version 4.0 (with Service Pack 5)		•	•	
Microsoft® Windows NT® version 4.0, Terminal Server Edition		•	•	
Microsoft® Windows NT® version 4.0, Enterprise Edition			•	
Microsoft® Windows® 2000 Server		•	•	
Microsoft® Windows® 2000 Advanced Server			•	

(continued)

**Table 2.1 Upgrade Paths for Windows XP Professional and Windows Server 2003**  
(continued)

Existing Operating System	Upgrade to Windows XP Professional	Upgrade to Windows Server 2003, Standard Edition	Upgrade to Windows Server 2003, Enterprise Edition	Upgrade to Windows Server 2003, Web Edition
Windows Server 2003, Standard Edition			●	
Windows 3.1				
Windows 95				
Windows 98	●			
Windows Millennium Edition	●			
Windows NT Workstation 4.0	●			
Windows 2000 Professional	●			
Microsoft® Windows XP Home Edition	●			

There are three exceptions to the options listed in Table 2.1:

- You cannot upgrade from one localized version of a Windows operating system to another localized version of a Windows operating system. For example, you cannot upgrade from the Japanese version of Windows 2000 Server to the English version of Windows Server 2003, Standard Edition.
- You can upgrade a computer that has the Multilingual User Interface Pack (MUI Pack) only to the English version of the operating system.
- You can upgrade from Windows NT 4.0 only if you have Service Pack 5 or later installed. It is not possible to upgrade a computer that has Windows NT 4.0 with Service Pack 4 or earlier.

## Evaluating Differences Between an Upgrade and a Clean Installation

During an upgrade, existing user settings are retained, as are installed applications and application settings. During a clean installation, the operating system files are installed in a new folder, and you must reinstall all of your applications and reconfigure user preferences, such as desktop and application settings.

The biggest benefit of an upgrade is that you can accommodate heterogeneous hardware and software configurations without having to customize individual computers in your organization. Also, because an upgrade does not affect applications, files, or settings, you do not have to spend time configuring computers or installing applications during a rollout, which speeds up the deployment process. Another benefit is that you do not need to migrate user data before an upgrade.

The biggest benefit of a clean installation is that all of your systems can be deployed with the same configuration. If you use the same answer file for all your systems during a clean installation, all applications, files, and settings are reset the same way, which means all of the desktops or servers in your organization can be standardized. In this way, you can avoid many of the support problems that are caused by irregular or inconsistent configurations.

You can use the following guidelines to determine whether to perform an upgrade or a clean installation.

Choose a clean installation if:

- No operating system is installed on the destination computer.
- The installed operating system cannot be upgraded to Windows XP Professional or Windows Server 2003.
- The computer has a multiple-boot configuration that needs to support the current operating system and either Windows XP Professional or Windows Server 2003.
- You are planning on implementing a managed environment through Group Policy, the Active Directory® directory service, or other means, but you have not yet implemented a managed environment. In this case, clean installations are desirable because they ensure that you have a standard configuration on which to implement your managed environment.
- You want to reset the desktop or server configuration in your organization to a consistent, known standard.
- You are purchasing new hardware or software as part of your deployment.

Choose to upgrade if:

- You already have a Windows operating system that is suitable for upgrading, and your IT department centrally manages the computers in your organization.
- You want to use existing hardware and software, and you do not want to reconfigure user settings, operating system settings, or application settings.
- You need to retain hardware or software settings for compatibility reasons.

You cannot use a distribution share to perform an unattended upgrade installation. You must use the product CD. Also, the Windows Setup program reads only a limited number of answer file sections and entries during an unattended upgrade installation. For more information, see “Performing an Unattended Upgrade Installation” later in this chapter.



### Important

Installing multiple operating systems on the same partition is not supported, and doing so can prevent one or both operating systems from working properly.

For a worksheet to help you record information about your installation, see “Unattended Installation Worksheet” (ACIUI\_1.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Unattended Installation Worksheet” on the Web at <http://www.microsoft.com/reskit>).

---

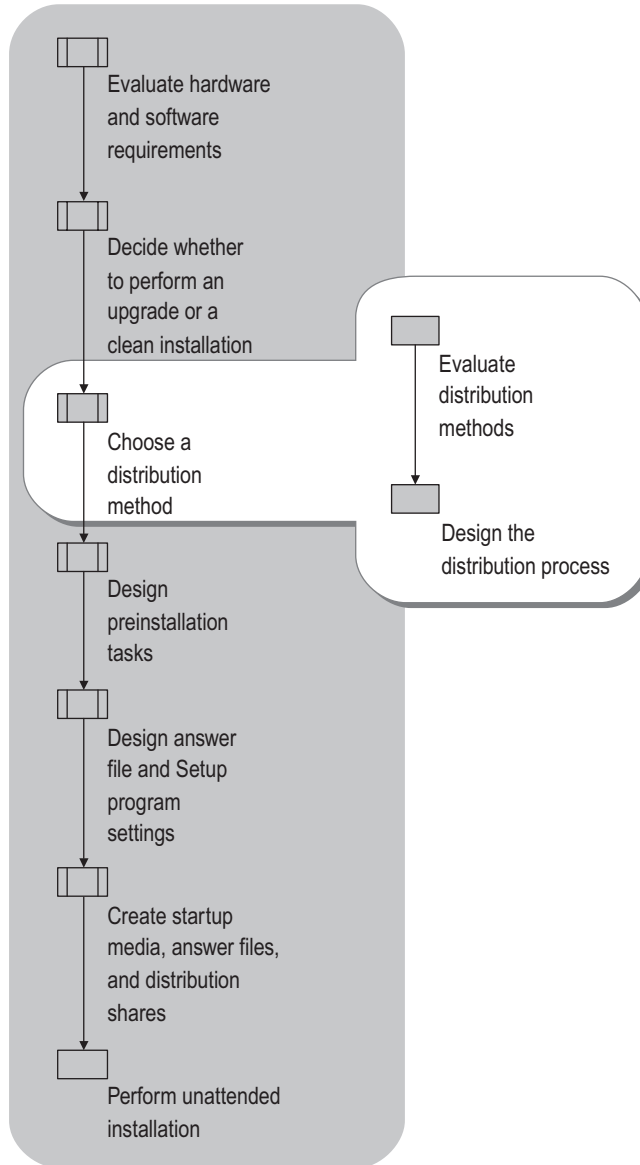
## Choosing a Distribution Method

*Distribution* refers to the way you store and transfer system files, device drivers, and software program files during an unattended installation. There are two types of distribution methods:

- You can store files in a distribution share on a network share, and then transfer the files across the network to each of the computers on which you are performing an unattended installation. This method works best when your destination computers are connected to a server by a reliable, high-bandwidth network.
- You can store files on media — such as a CD, a DVD, or a floppy disk — and then transfer the files locally from the media to each of the computers on which you are performing an unattended installation. Typically, when you use this method, you use the operating system CD in conjunction with a floppy disk. The operating system CD contains the system files and device drivers; the floppy disk contains the answer file that is necessary to perform an unattended installation.

Figure 2.4 shows the steps you need to follow to choose a distribution method for unattended installations.

**Figure 2.4 Choosing a Distribution Method**



## Evaluating Distribution Methods

Usually, unattended installations are performed with a distribution share. However, there are instances where a distribution share is not appropriate and you need to use media, rather than a distribution share, to perform an unattended installation. The guidelines in this section help you evaluate which distribution method is more appropriate for your organization's needs.

---

### Using a Distribution Share to Perform an Unattended Installation

A *distribution share* contains the Windows XP Professional or Windows Server 2003 installation files, as well as any device drivers or other files that are required to customize the installation. The distribution share is structured hierarchically and resembles the folder structure on a computer running Windows Server 2003 or Windows XP Professional. The folder typically resides on a server to which your destination computers can connect. You typically create one distribution share for each operating system you are deploying.

By using a distribution share to perform an unattended installation, you can perform the following tasks:

**Copy folders and files to destination computers** A distribution share can contain special folders and files that are copied to a computer's hard disk during an unattended installation. For example, if you want to create a Scripts folder on drive C of your destination computers, you can add the Scripts folder to your distribution share and it will automatically be copied to your destination computers during installation.

**Copy device drivers to destination computers** A distribution share contains folders for storing mass storage device drivers, HALs, and Plug and Play device drivers. The contents of these folders are copied to a computer's hard disk during an unattended installation.

**Copy a Sysprep folder to destination computers** A distribution share can contain a Sysprep folder, which can be used to store Sysprep files and the Sysprep.inf file. This is useful if you are performing image-based installations and you want to use unattended installation to create the master installations. In this case, you can add a Sysprep folder to the distribution share, and the Sysprep folder will automatically be created on the master installation when you perform an unattended installation.

Use a distribution share to perform your unattended installation if you want to:

- **Increase consistency.** When you use a distribution share, you create a single source for system files, device drivers, and customized installation files that are copied to each destination computer, which ensures that each unattended installation is consistent throughout your organization.
- **Reduce administrative costs.** All system files, device drivers, and customized installation files are stored in a central location, which reduces the cost of updating and changing system files and device drivers. For example, if you need to upgrade an existing device driver or add new device drivers, you only have to make the change in the distribution share. You do not need to create new answer files or create new floppy disks or CDs.

- **Control access to your installation files.** You can secure a distribution share by using file and folder permissions, which lets you specify the users and groups who can gain access to your installation files. By default, in Windows Server 2003, the Everyone group is granted read-only permissions when a folder is shared. Therefore, when you create a distribution share you need to grant write permissions to all of the users who are responsible for configuring the distribution share.

In addition, distribution shares are useful if you are performing other types of automated installations, such as image-based or RIS installations. In these cases, you can use unattended installation with distribution shares to create consistent master installations that are easily modified and updated.

Despite the advantages, there are several disadvantages that might preclude you from using a distribution share. If any of the following conditions are true, you probably do not want to use a distribution share to perform unattended installations:

- **Slow network connections.** Accessing a distribution share across a slow network connection, such as a dial-up connection or a slow wide area network (WAN) connection is overly time-consuming and impractical. It is recommended that you do not use a distribution share if your destination computers use a slow network connection to reach a distribution share.
- **Minimal file server capacity.** Distribution shares are typically stored on file servers. If your file servers do not have sufficient capacity to store all of your distribution shares, or if your file servers cannot handle an increase in file throughput during your rollout, then you cannot use a distribution share. The minimum disk space required for a distribution share for Windows Server 2003, Standard Edition is 650 megabytes (MB).
- **Minimal number of unattended installations.** You need to create, test, and maintain distribution shares. If you are performing only a few unattended installations, it is probably not cost-effective or efficient to use distribution shares. However, if you are performing image-based or RIS installations, and you are using unattended installations to create only a few master installations, distribution shares are useful and cost-effective because a distribution share ensures consistency among master installations and makes it easy to make configuration changes.

If you choose to use distribution shares, you can save the distribution shares on multiple servers. This allows Setup to copy files simultaneously from several servers, thereby speeding up the file copy stage of Setup. In addition, you can use Distributed File System (DFS) to increase the availability of your distribution shares. For more information about copying installation files from multiple servers, see “Choosing Winnt32.exe Parameters” later in this chapter. For more information about DFS, see “Designing and Deploying File Servers” in *Planning Server Deployments* of this kit.



## Using Media to Perform an Unattended Installation

Media distribution is useful if you are deploying computers in remote locations that do not have high-speed network connections, or in locations that do not have a local IT department available to set up and perform the unattended installation. Media distribution is also useful as an alternative installation method when network congestion limits your ability to access a distribution share, or when a destination computer has a malfunctioning network adapter.

To use media distribution instead of a distribution share, you use the operating system CD to start the destination computer. Then, you insert a floppy disk containing an answer file into the floppy disk drive. Setup reads the answer file, copies the appropriate installation files from the operating system CD to the destination computer's hard disk, and then configures the destination computer based on the parameters specified in the answer file.

Using an operating system CD to perform an unattended installation has the following requirements:

- The destination computer must have a bootable CD-ROM drive, and the boot-order sequence in the destination computer's BIOS must list the CD-ROM drive before the hard disk.
- The destination computer must have a floppy disk drive.
- The answer file must be named `Winnt.sif`, and it must be saved on a floppy disk.
- The installation files must all be present on the operating system CD; you cannot access supplemental device drivers or files that are not on the CD.
- The answer file must have a [Data] section, and the entries within the [Data] section must be configured appropriately for an unattended installation that uses an operating system CD.

In addition, using an operating system CD to perform an unattended installation has the following limitations:

- You cannot perform an upgrade, only a clean installation. To perform an upgrade, you must have an operating system running on the destination computer, which you do not have when you start a computer with the operating system CD.
- You cannot use a uniqueness database file (.udf) to modify the answer file. A .udf file overrides answer file settings, and is typically used to set the computer name during an unattended installation. For example, you might have a .udf file that contains a list of predetermined computer names for your organization. Instead of creating numerous answer files, each containing a unique computer name, you can configure the answer file so it obtains a computer name from the .udf file.

- You cannot use Dynamic Update to add updated installation files and device driver files during setup.
- You cannot stage the installation of applications. For more information about staging the installation of applications, see “Preinstalling Applications” in *Microsoft Windows Corporate Deployment Tools User’s Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.

Despite the requirements and limitations, there are some advantages to performing an unattended installation with the operating system CD. Namely, you can configure the answer file to do the following:

- **Configure disks.** By using the Repartition parameter in the [Unattended] section, you can delete all partitions on the destination computer and create a new partition that is formatted with the NTFS file system.
- **Skip Mini-Setup.** By using the UnattendSwitch parameter in the [Unattended] section, you can prevent the Mini-Setup program from running when the destination computer is started for the first time after unattended installation is completed.
- **Force BIOS startup.** By using the UseBIOSToBoot parameter in the [Data] section, you can force a destination computer to use the BIOS to start, even though Setup detects that it is more appropriate to use a device miniport driver to start the computer. The current generation of hardware uses the BIOS to start the computer, so this entry is rarely required. However, on computers with large drives that support extended int13 BIOS calls, this might not be the default behavior. Using the BIOS starts computers faster by eliminating possible delays caused by a miniport driver. Do not use this entry unless you are sure that the BIOS supports the extended int13 functions.

For more information about configuring an answer file for unattended installations, see “Designing Automated Installation Tasks” later in this chapter, and *Microsoft Windows Corporate Deployment Tools User’s Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.

## Designing the Distribution Process

After you choose a distribution method, you need to design the distribution process. If you use a distribution share to perform unattended installations, this includes designing the distribution share and determining which files and folders in the distribution share need to be renamed. If you use an operating system CD to perform unattended installations, this includes designing the startup process.

---

### Designing a Distribution Share

To design and configure a distribution share, you need to:

- **Structure the distribution share.** This includes identifying and structuring all of the supplemental files and folders that you want copied to the hard disk of each destination computer, such as device drivers, applications, and scripts.
- **Identify files that need to be renamed.** This includes files in the distribution share that need to be renamed after they are copied to a destination computer.

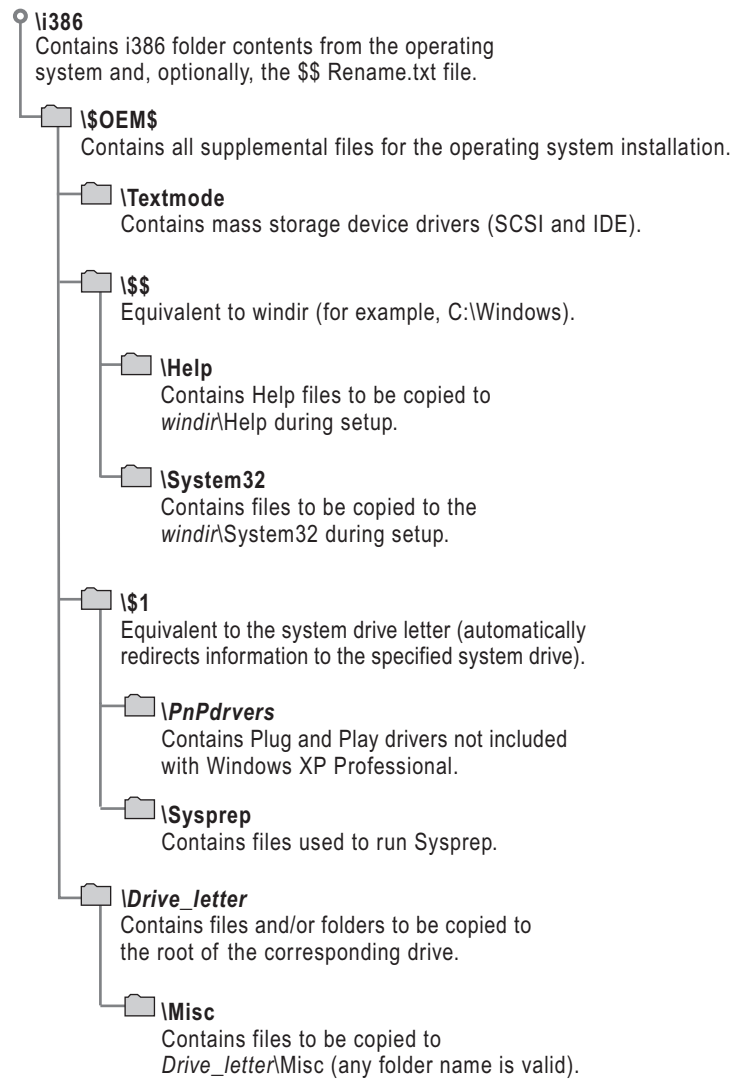
Three job aids are available to assist you with the design and configuration steps discussed in this section:

- For a worksheet to help you record information about the structure of your distribution share, see “Distribution Share Worksheet” (ACIUI\_2.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Distribution Share Worksheet” on the Web at <http://www.microsoft.com/reskit>).
- For a worksheet to help you record information about the files and folders in your distribution share that you need to rename, see “Renamed Files and Folders Worksheet” (ACIUI\_3.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Renamed Files and Folders Worksheet” on the Web at <http://www.microsoft.com/reskit>).
- For a worksheet to help you record general information about your unattended installation, including the location and name of your distribution share, see “Unattended Installation Worksheet” (ACIUI\_1.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Unattended Installation Worksheet” on the Web at <http://www.microsoft.com/reskit>).

## Structuring a Distribution Share

A distribution share consists of a single, top-level folder, named `i386`, and several subfolders. Figure 2.5 shows the structure of a distribution share.

**Figure 2.5 Distribution Share Structure**



**i386**

This is the distribution share. You create it at the root of the distribution server (the server on which the distribution share is located). You can use any name for this folder, but the name must not contain more than eight characters. You can create this folder by copying the contents of the i386 folder on a Windows Server 2003 or Windows XP Professional operating system CD.

**\$OEM\$**

You create the \$OEM\$ subfolder directly beneath the i386 folder. During setup, you can automatically copy folders, standard 8.3 format files, and any tools needed for your automated installation process to the \$OEM\$ subfolder.

If you want to create the \$OEM\$ subfolder outside the distribution share, you can use the OEMFILES\_PATH parameter in the answer file. For more information about answer file parameters and syntax, see *Microsoft Windows Corporate Deployment Tools User's Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.

The \$OEM\$ subfolder can contain the optional file Cmdlines.txt, which contains a list of commands to be run at the end of the graphical user interface (GUI)-mode stage of Setup. These commands can be used to install additional services or applications that you want to include with your installation. For more information about the Cmdlines.txt file, see “Designing Automated Post-Installation Tasks” later in this chapter.

As long as Setup finds the \$OEM\$ subfolder in the root of the distribution share, Setup copies all of the files found in this folder to the temporary directory on the destination computer that is created during the text mode stage of Setup.

**\$OEM\$\Textmode**

The \$OEM\$\Textmode subfolder contains new or updated files for installing mass storage device drivers and HALs. These files can include OEM HALs, drivers for SCSI devices, and Txtsetup.oem, which directs the loading and installing of these components. Be sure to include the Txtsetup.oem file. All files placed in the \$OEM\$\Textmode subfolder (HALs, drivers, and Txtsetup.oem) must be listed in the [OEMBootFiles] section of the answer file.

**\$OEM\$\\$\$**

The \$OEM\$\\$\$ subfolder is equivalent to the systemroot or windir environment variables. The subfolder contains additional files that you want copied to the various subfolders of the Windows Server 2003 or Windows XP Professional installation directory. The structure of this subfolder must match the structure of a standard Windows Server 2003 or Windows XP Professional installation, where \$OEM\$\\$\$ matches systemroot or windir (for example, C:\Windows), \$OEM\$\\$\$\Fonts matches windir\Fonts, and so on. Each subfolder must contain the files that need to be copied to the corresponding system folder on the destination computer.

**\$OEM\$\\$\$\Help**

A subfolder that contains the OEM Help files to be copied to the *systemroot*\Help folder during setup.

**\$OEM\$\\$\$\System32**

A subfolder that contains files to be copied to the *systemroot*\System32 folder during setup.

**\$OEM\$\\$1**

This folder points to the drive on which Windows Server 2003 or Windows XP Professional is installed; \$1 is equivalent to the *systemdrive* environment variable. For example, if you are installing Windows Server 2003 on drive D, \$OEM\$\\$1 points to drive D.

**\$OEM\$\\$1\Pnpdrivers**

You can use the \$OEM\$\\$1\Pnpdrivers subfolder to place new or updated Plug and Play device drivers in your distribution shares. These folders are copied to the *systemdrive*\Pnpdrivers location on the destination computer. Adding the *OemPnPDriversPath* parameter to your answer file directs Windows Server 2003 or Windows XP Professional to look (both during and after setup) for new or updated Plug and Play drivers in the folders that you created, in addition to those originally included with the system. Note that you can replace *Pnpdrivers* with a name of your own that is eight or fewer characters long.

**\$OEM\$\\$1\Sysprep**

The \$OEM\$\\$1\Sysprep subfolder is optional. This subfolder contains the files that you need to run Sysprep. For information about these files, see “Designing Image-based Installations with Sysprep” in this book.

**\$OEM\$\drive\_letter**

During the text mode stage of Setup, the structure and contents of each \$OEM\$\drive\_letter subfolder is copied to the root of the corresponding drive on the destination computer. For example, files that you place in the \$OEM\$\D subfolder are copied to the root of drive D. You can also create subfolders within these subfolders. For example, \$OEM\$\E\Misc causes Setup to create a subfolder called Misc on drive E.

**Tip**

If you are using MS-DOS to start the installation, and your MS-DOS-based tools cannot copy folders with path names longer than 64 characters, you can use short file names for the folders and then use *\$\$Rename.txt* to rename them later.

## Converting Short File Names to Long File Names by Using \$\$Rename.txt

If you are using Winnt.exe to perform an unattended installation, your distribution share can only contain files and folders that have short file names. This is because Winnt.exe only runs on MS-DOS, and MS-DOS can only process files and folders that use the 8.3 naming convention. The 8.3 naming convention allows only eight characters to the left of the decimal point and three characters to the right of the decimal point. Because of the short file name limitation, you need to shorten the names of files and folders so you can put them into your distribution share. You can convert these short file and folder names back to long file and folder names during setup by using the \$\$Rename.txt file.

\$\$Rename.txt lists all of the files and folders in a specific folder that need to be renamed. Each folder that contains short file names that need to be renamed must contain a separate version of \$\$Rename.txt. If you are using Winn32.exe to perform an unattended installation, short file names are automatically converted to long file names during setup.

To use \$\$Rename.txt, put the file in a folder that contains files and folders that need to be converted. Setup automatically looks for \$\$Rename.txt; if it finds a \$\$Rename.txt file, Setup renames the files in that folder. The syntax for \$\$Rename.txt is:

```
[section_name_1]

short_name_1 = "long_name_1"
short_name_2 = "long_name_2"
short_name_x = "long_name_x"

.
.
.

[section_name_2]

short_name_1 = "long_name_1"
short_name_2 = "long_name_2"
short_name_x = "long_name_x"

.
.
.
```

Where:

- *section\_name\_x* is the path to the folder that contains the files and folders. A section does not need to be named; it can have a backslash (\) as a name, which indicates that the section contains the names of the files or subfolders that are in the root of the drive.
- *short\_name\_x* is the name of the file or folder within this named folder that needs to be renamed. The name *must not* be enclosed in quotation marks.
- *long\_name\_x* is the new name of the file or folder. If the name contains spaces or commas, it *must* be enclosed in quotation marks.

## Designing the Media Distribution Process

If you plan to use an operating system CD to perform an unattended installation, you do not need to design a media distribution process. The installation files are already saved on the operating system CD, and you cannot change the structure of the operating system CD or add files to it. However, you do need to determine how to configure settings in the [Data] section of the answer file. Table 2.2 contains a description of these settings and guidelines to help you configure them. For a worksheet to help you record answer file settings, see “Answer File Settings Worksheet” (ACIUI\_5.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Answer File Settings Worksheet” on the Web at <http://www.microsoft.com/reskit>).

**Table 2.2 Answer File Settings for Installations That Use the Operating System CD**

Answer File Setting ([Section]/Entry)	Comment
[Data] AutoPartition = 1	Installs Windows on the first available partition that has adequate space for a Windows installation and does not already contain an installed version of Windows. Either omit the AutoPartition entry from your answer file or set the value of AutoPartition to 1. If AutoPartition is set to 1, the /tempdrive parameter of Winnt32.exe is ignored during setup. If you do not set the value, text mode stage of Setup installs Windows on the partition where \$WinIN_NTnt\$.~ls is located.
[Data] MsDosInitiated = 0	Informs the Windows Setup Loader that an unattended installation is running directly from the operating system CD. You must set this value to 0. If you do not set the value to 0, setup fails at the beginning of the GUI mode stage of Setup.
[Data] UnattendedInstall = Yes	Informs the Windows Setup Loader that an unattended installation is running directly from the operating system CD. You must set this value to Yes if you are installing Windows from the operating system CD.
[Data] UseBIOSToBoot = 0 or 1	Specifies whether Setup uses the BIOS to start the computer, even though Setup might detect that it is best to use a device miniport driver to start the computer. If you want to use the BIOS to start the computer, you must set this value to 1. The default setting is 0. Do not use this entry unless you are sure that the BIOS supports the extended int13 functions.

(continued)



**Table 2.2 Answer File Settings for Installations That Use the Operating System CD**  
(continued)

Answer File Setting ([Section]/Entry)	Comment
[Unattended] Repartition = Yes or No	Specifies whether to delete all partitions on the first drive of the destination computer and to reformat the drive with NTFS. The default setting is No. Change this to Yes if you want the installation to manually run the GUI mode stage of Setup (the text mode stage of Setup is automated, but the GUI mode stage of Setup is not). If you leave the default setting, and Setup detects a Windows installation on the first drive of the destination computer, Setup will stop during the text mode stage of Setup and ask you whether you want to delete the existing Windows installation.
[Unattended] UnattendSwitch = Yes or No	Specifies whether Setup skips Mini-Setup when installing Windows XP Professional or Windows Server 2003. Use only with Winnt.exe. The default setting is No.

For more information about answer file settings, see *Microsoft Windows Corporate Deployment Tools User's Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.

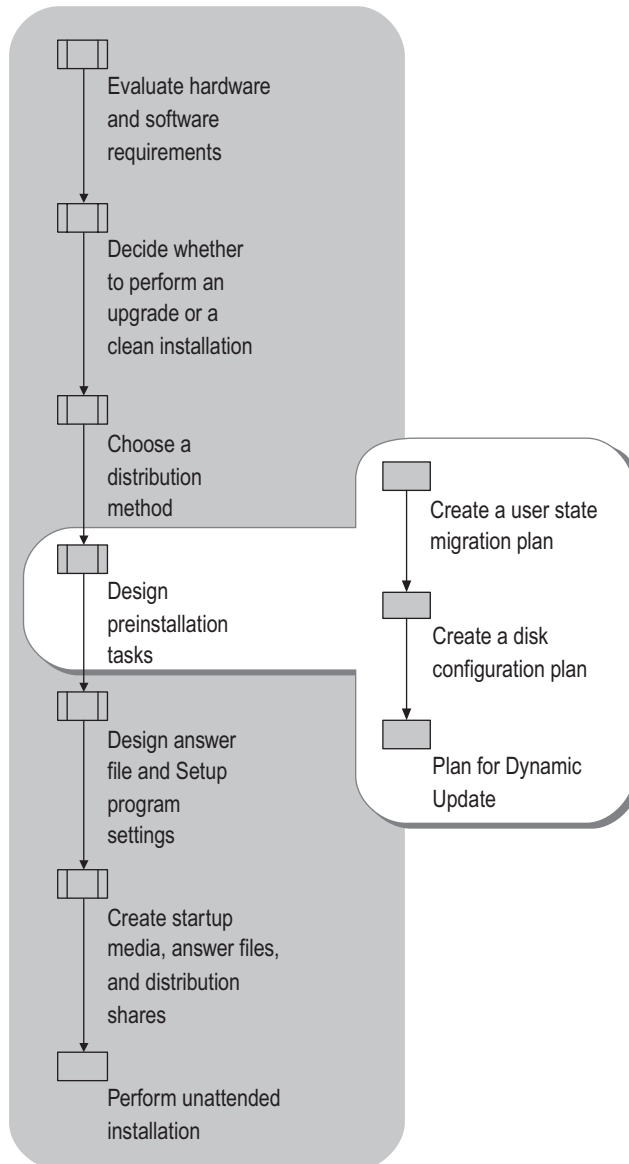
## Designing Preinstallation Tasks for Unattended Installations

After you determine which distribution method to use, you need to identify your preinstallation tasks. Preinstallation tasks are performed before you begin an unattended installation. You might not need to perform any preinstallation tasks; you will need to perform some preinstallation tasks if you want to:

- Migrate user state before you perform an unattended installation. When you migrate user state, you save user settings and user data on some type of external media so you can restore the settings and data after the unattended installation is complete. You will likely not need to do this if you use folder redirection and roaming profiles to store user data and settings on a server. For more information about roaming profiles, see “Using roaming user profiles” in Help and Support Center for Windows Server 2003. For more information about folder redirection, see “Designing a Group Policy Infrastructure” in *Designing a Managed Environment* of this kit.
- Change the size or format of the system partition before you perform an unattended installation.
- Use Dynamic Update to download updated installation files and device drivers with your unattended installation.

Figure 2.6 shows the design steps you need to follow to design your preinstallation tasks.

**Figure 2.6 Designing Preinstallation Tasks**



## Creating a User State Migration Plan for Unattended Installations

You will need to create a user state migration plan if any of your destination computers contain any of the following items that you want to restore after installation is complete:

- User data that you want to be available to the end user. User data includes such things as documents, e-mail messages, spreadsheets, and databases.
- User settings, such as desktop settings, shortcuts, and Internet Explorer Favorites.
- Application settings such as application-specific keyboard shortcuts, spell-checking options, and default file locations.

At a minimum, your user state migration plan must do the following:

- Identify the data you want to migrate, including user data, user settings, and application settings.
- Describe how to collect and restore the data.
- Determine where to store the data while you perform the unattended installation.
- Create a schedule for migrating the data on each of your destination computers.

Microsoft provides two tools for migrating user data and settings. The tool you use depends on your environment:

- **Files and Settings Transfer Wizard.** Designed for home users and small office users, the 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 Helpdesk.
- **User State Migration Tool.** Designed for IT administrators who perform large deployments of Windows XP Professional in a corporate environment, the User State Migration Tool provides the same functionality as the wizard, but on a large scale targeted at migrating multiple users. The User State Migration Tool gives administrators command-line precision for customizing specific settings, such as unique modifications to the registry. To download a free version of the tool, see the User State Migration Tool link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

For more information about migrating user data and settings, see “Migrating User State” in this book. Also see the articles “User State Migration in Windows XP,” “Step-by-Step Guide to Migrating Files and Settings,” “Deploying Windows XP Part I: Planning,” and “Deploying Windows XP Part II: Implementing.” To find these articles, see the Microsoft TechNet link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

## Creating a Disk Configuration Plan for Unattended Installations

You need to create a disk configuration plan if you need to do any of the following before you perform the installation:

- Change the size of the system partition on your destination computers.
- Repartition and reformat the system partition on your destination computers, and you are not using an operating system CD to start your destination computers.
- Create and format extra partitions on your destination computers.

You do not need to create a disk configuration plan in the following situations:

- You want to extend the system partition, create and format extra partitions during or after the installation, or convert an existing system partition to NTFS. These tasks do not require substantial analysis and planning, and are relatively easy to perform by configuring answer file settings or running commands or scripts from the answer file.
- You are using an operating system CD to perform an unattended installation, and you want to repartition and format the system partition on destination computers. In this case, you can use the Repartition entry in the [Unattended] section of the unattended installation answer file to repartition and format the system partition before the unattended installation begins.

### Configuring Disk Settings

Begin your disk configuration plan by choosing the tool that most suits your needs:

#### MS-DOS or Windows 98 disk configuration tools

You can start a destination computer by using an MS-DOS or a Windows 98 boot disk, and then use the **fdisk** and **format** commands to partition and format the hard disk before you perform an unattended installation. This works only if you want to format your disks with the FAT or FAT32 file systems. If you want your hard disks formatted with NTFS, you will have to use the **convert** command to convert the FAT or FAT32 file system to NTFS after you have installed the operating system onto the destination computer, or you will have to use the **oformat** command. For more information about disk tools, including commands for configuring disks, see “Helpful Command Line Tools” in the *Microsoft Windows Corporate Deployment Tools User’s Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD. For more information about disk partitions and file systems, see the *Server Management Guide* of the *Microsoft® Windows® Server 2003 Resource Kit* (or see the *Server Management Guide* on the Web at <http://www.microsoft.com/reskit>).

### Third-party disk configuration tools

Some third-party disk management programs provide a bootable floppy disk or CD that allows you to partition and format hard disks. If you use a third-party program to partition or format a disk, be sure that the third-party program creates partitions that are compatible with NTFS 3.1, which is the version of NTFS that is used in Windows XP Professional and Windows Server 2003 operating systems.

### Windows Preinstallation Environment

You can start a destination computer by using a Microsoft® Windows® Preinstallation Environment (Windows PE) CD, and then using the **diskpart** command to partition the hard disk and the **format** command to format the hard disk. Windows PE is a bootable operating system that provides limited operating system functionality for performing preinstallation tasks. Windows PE is available only if you have purchased Enterprise Agreement 6.0, Enterprise Subscription Agreement 6.0, or Select License 6.0 with Software Assurance (SA). For more information about Windows PE and Windows PE licensing plans, see the Windows Preinstallation Environment link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

Each method of configuring disk settings has advantages and disadvantages. You need to determine which method is better suited to your organization and your deployment needs. For more information about configuring disks, see “Disk Management overview” in Help and Support Center for Windows Server 2003.

## Components of a Disk Configuration Plan

After you determine which method to use to configure disk settings, you need to create your disk configuration plan. At a minimum, your disk configuration plan must identify:

- **Disk configuration settings.** Disk configuration settings include the number of partitions, partition sizes, and file system formats for the destination computer. Disk configuration settings are based on several factors, including disk sizes, disk types, backup capabilities, and user needs. Analyze these factors in your disk configuration plan to determine the right disk configuration for your organization.
- **Procedures for configuring disk settings.** Your disk configuration plan must describe every step of the disk configuration process, including how to start a destination computer and how to run the partitioning or formatting tools.
- **Tools that you use to configure disk settings.** Disk configuration tools include the **format**, **fdisk**, and **diskpart** commands. Your disk configuration plan must describe all the tools you will use to configure disk settings, including the tools you will use to start a destination computer and to partition, format, and check a disk.

## Planning for Dynamic Update

You can use Dynamic Update to update installation files and device drivers that are used by Setup during an unattended installation. Dynamic Update does not replace Windows Update; it downloads only a small subset of Windows Update files and device driver files that prevent critical errors from occurring during the setup process. The files that Dynamic Update downloads include:

- **Updated installation files.** This can include system files, in-box device drivers, Setup information (.inf) files required during upgrades, DLL files used by the Winnt32.exe Setup program, and file assemblies (.asm files). Dynamic Update downloads only replacements for existing installation files. It does not add new installation files to the setup process.
- **New device drivers.** This can include new device drivers that are critical to the setup process and are not on the operating system CD. New device driver files are not replacements for in-box device drivers. Replacements for in-box device drivers are considered updated installation files.

You can use Dynamic Update only if you are installing on destination computers that have an existing connection to your network or the Internet. For example, you can use Dynamic Update if your destination computer is running Windows 2000 and it is connected to your network when you run Windows Setup. In addition, you can use Dynamic Update only with Winnt32.exe; you cannot use Dynamic Update with Winnt.exe. By default, Dynamic Update is disabled during an unattended installation of Windows Server 2003 and Windows XP Professional.

In addition, if you are upgrading a computer that is running Windows 95 with Internet Explorer 4.01, you need to upgrade to Internet Explorer 5.0 or a higher version of Internet Explorer. The version of Secure Sockets Layer (SSL) in Internet Explorer 4.01 is not compatible with Dynamic Update, and will cause Dynamic Update to fail.

### Delivering Dynamic Update files to destination computers

You can deliver Dynamic Update files to destination computers two ways: you can download Dynamic Update files across the Internet from the Windows Update Web site, or you can download Dynamic Update files across your corporate network from a shared folder that you create on a server in your organization. The latter method is better suited for large-scale corporate deployments because it ensures consistency among your destination computers.

When you download Dynamic Update files from a server in your organization, you can guarantee that the same set of Dynamic Update files are downloaded onto each of your destination computers because you have full control of the Dynamic Update files that are on the server. When you download Dynamic Update files across the Internet from the Windows Update Web site, you might introduce inconsistencies among your destination computers because the Windows Update Web site is periodically updated, and you cannot control when this occurs. In addition, downloading Dynamic Update files from a server in your organization eliminates many security issues that can arise when destination computers are connected to the Internet.

**Note**

This book assumes you are delivering Dynamic Update files across your corporate network from a server in your organization. This book does not describe how to configure an unattended installation so that Dynamic Update files are delivered across the Internet.

**Preparing to use Dynamic Update**

To use Dynamic Update, you need to determine the following:

- Which files to deliver to your destination computers.
- How to prepare the files for delivery.
- How to configure answer files settings or Winnt32.exe settings.

For a worksheet to help you record information about your Dynamic Update design, see “Dynamic Update Worksheet” (ACIUI\_4.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Dynamic Update Worksheet” on the Web at <http://www.microsoft.com/reskit>).

---

## Identifying and Downloading Dynamic Update Files

You need to download two types of files to prepare for Dynamic Update: Dynamic Update packages, which contain updated installation files; and device driver .cab files, which contain new device driver files that are not present on the operating system CD. Device driver files must be downloaded individually; they are not assembled in packages.

**Downloading Dynamic Update Packages**

You can download Dynamic Update packages from the Microsoft Download Center. To do this, go to the Microsoft Download Center, specify the operating system that you are deploying, and then search for the keywords “dynamic update.” Download the most current Dynamic Update package (the Dynamic Update package with the highest version number). To use the Microsoft Download Center, see the Microsoft Download Center link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

For information about downloading the most recent Dynamic Update package for Windows XP Professional, see article Q311220, “Description of the Dynamic Update Feature in Windows XP Setup,” 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 about downloading the most recent Dynamic Update package for Windows Server 2003, search the Microsoft Knowledge Base using the keywords “dynamic update.”

### **Downloading device driver files**

You can download new device driver .cab files from the Windows Update corporate Web site. Before you do this, you need to identify all of the devices on your destination computers for which there are no device drivers on the operating system CD. To identify these devices, use an operating system CD to manually install the operating systems you are deploying on a representative sampling of your destination computers. You can then use Device Manager to check the device status for each device. Devices that do not have device drivers are denoted with a yellow question mark and a yellow exclamation mark in Device Manager. To download device driver .cab files, see the Windows Update link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.



### **Important**

Use Dynamic Update to install missing device drivers only for devices that are critical for Setup, such as hard disk controllers, mice, display adapters, and keyboards. Do not use Dynamic Update to install missing device drivers for peripheral devices, such as scanners, cameras, and printers. To install missing device drivers for peripheral devices, or devices that are not critical for Setup, use the OemPnPDriversPath entry in the [Unattended] section of your answer file.

---

## **Preparing Dynamic Update Files**

After you download the Dynamic Update packages and the device driver .cab files, you need to prepare these files for delivery to your destination computers. Perform the following tasks to prepare Dynamic Update files.

### **Extract the Dynamic Update packages**

Run the executable Dynamic Update package to extract the Dynamic Update files. This creates separate folders for each operating system. For example, if you run the executable Dynamic Update package for Windows XP, this creates two folders: a Windows XP Professional folder named IP, and a Windows XP Home Edition folder named IC. If you run the executable Dynamic Update package for Windows Server 2003, this creates three folders in your new folder: a Windows Server 2003, Standard Edition folder named Standard; a Windows Server 2003, Enterprise Edition folder named Enterprise; and a Windows Server 2003, Web Edition folder named Web. Each folder can contain one or more of the following files: Winnt32.cab, Updates.cab, Upginf.cab, Duasms.cab. Delete the folders for any operating systems that you are not installing. For example, if you are not installing Windows XP Home Edition, delete the IC folder.



**Copy the .cab files to new folders**

Copy the .cab files for each operating system, and each of the new device driver .cab files for each operating system, to a new folder. For example, copy the .cab files in the IP folder to a folder named DU\_XPPro, and copy any new device driver files you downloaded for Windows XP Professional to the DU\_XPPro folder.

**Use the /dupprepare parameter to prepare each folder**

Run Winnt32.exe with the **/dupprepare** parameter on each of the new folders. This prepares each folder for Dynamic Update. During the preparation process, Winnt32.exe creates one or more of the following subfolders: Duasms, Dudrvs, Updates, Upginfs, and Winnt32. Winnt32.exe also copies the contents of the .cab files to one or more of these subfolders.

For more information about preparing files for Dynamic Update, see article Q312110, “How to Deploy the Windows XP Dynamic Update Package,” 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>.

**Configure a Shared Folder for Dynamic Update files**

To distribute Dynamic Update files across your corporate network, you need to create a shared folder on a server. The shared folder must be available to all of your destination computers. For example, do not create the shared folder on a server that is in a restricted subnet. Typically, you create the shared folder on the same server that contains your distribution shares.

In addition, you need to assign permissions to the shared folder. If you create the shared folder on the same server that contains your distribution shares, the shared folder should have the same permissions as your distribution shares. Permissions ensure that only authorized users can access the shared folder. If the shared folder is not secure, a malicious user could tamper with the Dynamic Update files. For example, a malicious user could replace the .cab files in the shared folder with .cab files that contain a virus. For more information about permissions, see “Best practices for permissions and user rights” in Help and Support Center for Windows Server 2003.

**Copy the prepared Dynamic Update Files to the shared folder**

After you create the shared folder on a server, copy each of the prepared Dynamic Update folders to it. The “Dynamic Update Worksheet” (ACIUI\_4.doc) shows the structure of the shared folder, and provides spaces for you to record the names of the folders containing your Dynamic Update files. See “Dynamic Update Worksheet” (ACIUI\_4.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Dynamic Update Worksheet” on the Web at <http://www.microsoft.com/reskit>). You will need the names of these folders to design your answer file settings and Setup program settings later in this chapter.

## Configuring Answer File and Winnt32.exe Settings for Dynamic Update

Dynamic Update is disabled by default when you perform an unattended installation with an answer file. Dynamic Update is enabled by default when you perform an unattended upgrade installation by running **Winnt32.exe /unattend**.

To use Dynamic Update during an unattended installation with an answer file, you need to add the following entry to the [Unattended] section of your answer file:

```
DUDisable=No
```

This entry tells Setup to enable Dynamic Update. By default, this entry is set to Yes, which means Dynamic Update is disabled.



### Important

Do not use the `/dudisable` parameter with Winnt32.exe if you enable Dynamic Update in your answer file. The `/dudisable` parameter takes precedence over the DUDisable entry in your answer file: that is, using the `/dudisable` parameter disables Dynamic Update regardless of how you configure your answer file.

In addition, you need to specify the location of the shared folder that contains the prepared Dynamic Update files. You can do this by creating the following entry in the [Unattended] section of your answer file:

```
DUShare = path_to_prepared_dynamic_update_files
```

You can also do this by using the following command-line parameter with Winnt32.exe:

```
/DUShare:path_to_prepared_dynamic_update_files
```

In both cases, *path\_to\_prepared\_dynamic\_update\_files* is the path to the folder containing the Dynamic Update files that you downloaded, prepared, and saved on a secure shared folder in your organization. This path is different for each operating system you are installing.

In addition, when you perform an unattended installation, you can change the way Setup responds to Dynamic Update errors by using the DuStopOnError parameter in the [Unattended] section of your answer file. Dynamic Update errors include any failure to process Dynamic Update files, or the inability to connect to Windows Update. By default, the Dynamic Update process stops when an error is detected. You can change this by adding the following entry to your answer file:

```
DuStopOnError=No
```

For a worksheet to help you record answer file information, see “Answer File Settings Worksheet” (ACIUI\_5.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Answer File Settings Worksheet” on the Web at <http://www.microsoft.com/reskit>). For more information about answer file settings and Winnt32.exe parameters, see *Microsoft Windows Corporate Deployment Tools User's Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.

---

# Designing Answer File and Setup Settings for Unattended Installations

By creating an answer file and by using Setup command line parameters, you can automate the following tasks that occur during and after an unattended installation:

- **Software installation and configuration.** You can automatically install and configure client and server applications. You also can install and configure Windows components, services, and applications.
- **Hardware installation and configuration.** You can automatically update device drivers and configure device settings.
- **Computer configuration.** You can automatically configure computer settings, such as domain membership, computer name, network protocols, display settings, and system services. You also can configure server roles, such as installing Active Directory.

Try to automate as many installation and post-installation tasks as possible during an unattended installation. By automating installation and post-installation tasks, you can:

- Reduce the number of errors caused by technicians, administrators, and end users during your deployment.
- Ensure consistency throughout your organization, which reduces support costs after deployment.
- Increase productivity by requiring little or no end-user interaction during your deployment.
- Update or modify your installation process without having to educate or retrain end users, technicians, or administrators.

To automate installation and post-installation tasks, you need to create and configure an answer file. In addition, you need to choose which command line parameters to use when you start the Setup program.

The answer file for unattended installations of Windows Server 2003 and Windows XP Professional is usually named `Unattend.txt`, but you can name it anything you want. However, if you start a destination computer from an operating system CD and the answer file is on a floppy disk, you must name the answer file `Winnt.sif`. Setup will then detect the answer file on the disk without user input.

The answer file supplies Setup with answers to all the questions that you are asked during a standard, interactive installation. The answer file also contains information about your installation and configuration requirements. In addition, an answer file tells Setup how to interact with the distribution shares and files that you have created (or the installation files on the operating system CD, if that is what you are using to install the product).

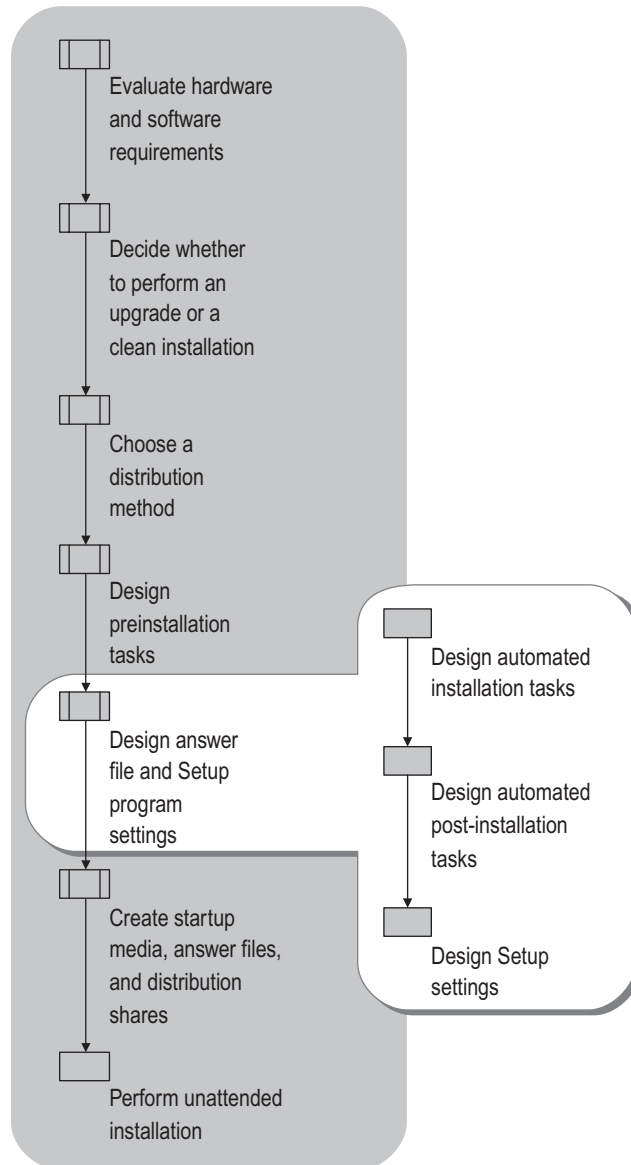
An answer file contains multiple sections — some mandatory and some optional — that you can modify. Section names are delineated by brackets (for example, `[Unattended]`). Every section has one or more entries that contain installation and configuration information. Entries are delineated by an entry name, an equal sign, and a value (for example, `ComputerName = Computer1`). The entry name represents a specific computer setting or action; the value represents the unique way you want the setting configured or the action performed. For more information about answer file sections and entries, see “`Unattend.txt`” in the “Reference” section of the *Microsoft Windows Corporate Deployment Tools User’s Guide* (`Deploy.chm`). `Deploy.chm` is included in the `Deploy.cab` file in the Support folder on the Windows Server 2003 operating system CD.

Setup parameters are specified at the command line when you run `Winnt.exe` or `Winnt32.exe`.

Some installation and configuration tasks can be performed by configuring either Setup parameters or answer file settings. For example, you can implement Dynamic Update by configuring answer file settings or by configuring Setup parameters when you run `Winnt32.exe`. In both cases, the functionality is the same. For more information about Setup, see “Using `Winnt.exe` to Run Setup” and “Using `Winnt32.exe` to Run Setup” in the *Microsoft Windows Corporate Deployment Tools User’s Guide* (`Deploy.chm`). `Deploy.chm` is included in the `Deploy.cab` file in the Support folder on the Windows Server 2003 operating system CD.

Figure 2.7 shows the design process you need to follow to automate tasks during an unattended installation.

**Figure 2.7 Designing Answer Files and Setup Parameters**



## Designing Automated Installation Tasks

To design automated installation tasks for an unattended installation, you must identify:

- The installation tasks you want to automate.
- The settings you need to configure for the answer file.

Installation tasks are usually described in your component design or your client and server configuration design. For example, your network topology should provide information about the network protocol settings you need to configure during an installation. Likewise, your file server design should provide information about the disk settings you need to configure during an installation.

Answer file settings correspond to the installation tasks you need to perform. For example, if one of your installation tasks involves configuring network adapter settings, you need to identify the answer file sections and entries that configure network adapter settings, and then determine the proper values to assign to the answer file entries.

### Identifying Automated Installation Tasks

Use Table 2.3 to determine which installation tasks you can automate by configuring an answer file. Try to automate as many installation tasks as possible with the answer file.

**Table 2.3 Tasks You Can Automate with an Unattended Installation Answer File**

Installation Task	Comments
Hardware installation and configuration	This includes installing and configuring mass storage controllers that are required at startup, such as SCSI hard disks and Plug and Play devices that are not included on the operating system CD.
Setup configuration	This includes partitioning and formatting hard disks prior to setup, and configuring Setup options that are usually configured by end users during GUI mode and text mode stage of Setup. This also includes configuring upgrade options, uninstall options, and other settings that affect the way Setup runs.
Operating system configuration	This includes configuring power management, telephony, and display settings, and regional options. This also includes configuring error reporting, Windows file protection, remote assistance, system restore, licensing, and shell settings.
Internet Explorer configuration	This includes configuring Internet Explorer options, such as favorites, proxy server settings, branding, and default Home and Search pages. Also includes configuring Internet Explorer Enhanced Security Configuration settings.*

(continued)

**Table 2.3 Tasks You Can Automate with an Unattended Installation Answer File (continued)**

Installation Task	Comments
Networking configuration	This includes configuring Internet Connection Sharing (ICS), Internet Connection Firewall (ICF), and domain membership settings. This also includes installation and configuration of protocols, network adapters, and networking services and components.
Services configuration	This includes configuring Internet Information Services (IIS), Certificate Services, Remote Installation Services, Terminal Server, fax service, and Simple Network Management Protocol (SNMP) service. This also includes installing and configuring a domain controller by using Active Directory.
Optional Windows components and services installation	This includes all Windows components listed in Add or Remove Programs in Control Panel, such as accessories, games, media services, and Indexing Service.
Software application installation and configuration	This includes Windows Installer (.msi) packages and staged software. Software installation must run in quiet mode, which means the installation must be fully automated and cannot rely on user interaction. Usually, when you run an installation program in quiet mode, you must provide an answer file.
Running programs, scripts, and batch files	Programs, scripts, and batch files must be fully automated and cannot rely on user interaction, which means you must provide an answer file for any programs, scripts, or batch files you are running, and you must be able to run the programs, scripts, or batch files in quiet mode.

\* For more information about Internet Explorer Enhanced Security Configuration settings, see "Internet Explorer Enhanced Security Configuration" in Help and Support Center for Windows Server 2003. For more information about answer file settings related to Internet Explorer Enhanced Security Configuration, see the Readme.txt file in Deploy.cab. Deploy.cab is in the Support folder on the Windows Server 2003 operating system CD.

## Identifying Answer File Settings

Use Table 2.4 to find the specific answer file section that corresponds to each installation task. For a Word document to assist you in recording your answer file settings, see “Answer File Settings Worksheet” (ACIUI\_5.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Answer File Settings Worksheet” on the Web at <http://www.microsoft.com/reskit>).

**Table 2.4 Installation Tasks and Corresponding Answer File Sections**

To Automate This Task	Configure These Answer File Sections
Hardware installation and configuration	[MassStorageDrivers] [OEMBootFiles] [Unattended]
Setup configuration	[Data] [GuiUnattended] [Unattended] [Win9xUpg]
Operating system configuration	[Display] [LicenseFilePrintData] [PCHealth] [RegionalSettings] [Shell] [SystemFileProtection] [SystemRestore] [TapiLocation] [UserData]
Internet Explorer configuration	[Branding] [FavoritesEx] [Proxy] [URL] [Components] [IEHardening]

(continued)



**Table 2.4 Installation Tasks and Corresponding Answer File Sections (*continued*)**

To Automate This Task	Configure These Answer File Sections
Networking configuration	[Homenet] [Identification] [MS_AppleTalk parameters] [MS_ATMArps parameters] [MS_ATMLANE parameters] [MS_ATMUni parameters] [MS_L2TP parameters] [MS_MSCClient parameters] [MS_NetMon parameters] [MS_NWClient parameters] [MS_NWIPX parameters] [MS_NwSapAgent parameters] [MS_PPTP parameters] [MS_Psched parameters] [MS_RAS parameters] [MS_RasSrv parameters] [MS_Server parameters] [MS_TCPIP parameters] [MS_WLBS parameters] [NetAdapters] [NetBindings] [NetClients] [NetOptionalComponents] [NetProtocols] [NetServices] [Networking]
Services configuration	[DCInstall] [Fax] [InternetServer] [OsChooser] [RemoteInstall] [SNMP] [TerminalServices] [CertSrv_Client] [CertSrv_Server]

**(continued)**

**Table 2.4 Installation Tasks and Corresponding Answer File Sections (continued)**

To Automate This Task	Configure These Answer File Sections
Optional Windows components and services installation	[Components]
Software application installation and configuration	[GuiRunOnce] [SetupParams]
Running programs, scripts, and batch files	[GuiRunOnce] [SetupParams]

Most answer file settings are optional; however, if you want a fully automated unattended installation, you must configure the following sections and entries in your answer file. If you do not provide values for these entries in your answer file, Setup will prompt the end user (or whoever is performing the unattended installation) for the values:

**[GuiUnattended]** You must specify values for AdminPassword and TimeZone. The value for AdminPassword cannot begin with an asterisk (\*). Using a password that begins with an asterisk can cause the password to be set to a null value.

**[Identification]** You must specify values for JoinDomain, DomainAdmin, and DomainAdminPassword.

**[LicenseFilePrintData]** You must specify values for AutoMode and AutoUsers if you are installing a Windows Server 2003 product.

**[Networking]** If your destination computer requires network connectivity, you must specify values for various network protocol entries.

**[Unattended]** You must specify values for UnattendMode and TargetPath.

**[UserData]** You must specify values for FullName and ComputerName.

For more information about specific answer file settings — including procedural and reference information about creating, formatting, and configuring an answer file for unattended installation — see *Microsoft Windows Corporate Deployment Tools User's Guide* (Deploy.chm).

Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.

## Designing Automated Post-Installation Tasks

Post-installation tasks include any installation and configuration tasks that need to be performed after the operating system is installed. Post-installation tasks are usually described in your component design or your client and server configuration design. You usually perform these tasks by running a command, program, script, or batch file after Setup is finished running. For example, your client networking design might include information about network settings that need to be configured with the Netset.exe command line tool. Likewise, your client configuration design might include information about mapped network drive settings that need to be configured with the **net use** command or printers that need to be installed with the Rundll32.exe program.

You can automate these types of tasks after the operating system is installed by using a Cmdlines.txt file or by using the [GuiRunOnce] section in your answer file. Both methods allow you to run commands, programs, scripts, and batch files.

To design automated post-installation tasks for an unattended installation, you must:

- Identify the tasks you want to perform after the operating system is installed.
- Design a method for automating the tasks you want to perform.

---

## Identifying Automated Post-Installation Tasks

You can use an answer file to automate only a limited number of installation and configuration tasks during installation. Many installation and configuration tasks must be performed after the operating system is installed and configured. Testing your unattended installations is the best way to determine whether an installation or configuration task must be performed after the operating system is installed. However, the following installation and configuration tasks always must be performed after the operating system is installed:

- Tasks that cannot be performed by setting an answer file entry. You cannot add any other sections or entries to an answer file that is used to perform an unattended installation. For a worksheet that contains a list of all possible answer file sections and entries, see “Answer File Settings Worksheet” (ACIUI\_5.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Answer File Settings Worksheet” on the Web at <http://www.microsoft.com/reskit>).
- Tasks that rely on Active Directory directory service. For example, if a software installation program registers information in Active Directory or requires information from Active Directory, you must run the installation program after the operating system is installed and the computer is joined to a domain.
- Tasks that can be performed only while a user is logged on. For example, some software installation programs create shortcuts on the **Start** menu and the desktop. If you want these shortcuts applied to a specific user profile, then you need to run the installation program after the operating system is installed and the user is logged on.

You can automate post-installation tasks only if you can run the command, program, script, or batch file in quiet mode, or if you can suppress all user prompts by supplying an answer file for the command, program, script, or batch file. For example, if you delete folders after you install the operating system, you need to use the **/q** parameter with the **rmdir** command. Likewise, if you install Microsoft Word after you install the operating system, you need to create a Setup.ini file that provides configuration information to the Word Setup program.

---

## Choosing a Method for Automating Post-Installation Tasks

You can perform automated post-installation tasks two ways: you can use a Cmdlines.txt file to run commands, programs, scripts, or batch files just after Setup finishes but before the computer restarts, or you can configure the [GuiRunOnce] section in an answer file to run commands, programs, scripts, and batch files after the computer restarts and a user logs on. Use the following guidelines to determine which method to use.

### Using Cmdlines.txt

Use Cmdlines.txt when:

- You are running commands, programs, scripts, or batch files from the \$OEM\$ folder on a distribution share.
- You want to install applications or perform configuration tasks during GUI mode stage of Setup.
- You want to install applications or perform configuration tasks under the Local System security account.
- You do not need network connectivity to perform the installation or configuration task.
- You are not using Windows Installer packages (.msi files) to install applications.
- You want to install applications or perform configuration tasks while no user is logged on.

### Using [GuiRunOnce]

Use [GuiRunOnce] when:

- You need access to hard drives, CD-ROM drives, shared folders on the network, or other storage devices.
- You want to install applications or perform configuration tasks under a specific user account.
- You need network connectivity to perform an installation or configuration task.

- You are using Windows Installer packages (.msi files) to install applications.
- You need to control the order in which programs, scripts, or batch files run.



### Important

You cannot use Cmdlines.txt if you are using an operating system CD and a Winnt.sif file to perform an unattended installation. You can use Cmdlines.txt only if you are installing from a distribution share.

For information about configuring Cmdlines.txt and [GuiRunOnce] to run programs, scripts, and batch files, see “Configuring Cmdlines.txt to Perform Tasks” and “Configuring [GuiRunOnce] to Perform Tasks” later in this chapter.

## Configuring Cmdlines.txt to Perform Tasks

The Cmdlines.txt file contains a list of commands, programs, scripts, or batch files that are executed at the end of GUI mode stage Setup. You can configure Cmdlines.txt to run multiple commands, programs, scripts, or batch files. The commands, programs, scripts, and batch files run synchronously; for example, a command waits for the previous command to finish running before it starts. This means that you can control the order in which commands, programs, scripts, and batch files run. By default, Cmdlines.txt is not created, so you must manually create the file and save it in the \$OEM\$ folder in your distribution share.

The syntax for Cmdlines.txt is as follows:

```
[Commands]
```

```
"command_1"
```

```
"command_2"
```

```
.
```

```
.
```

```
"command_x"
```

Where *command\_1*, *command\_2*, and *command\_x* refer to the commands, programs, scripts, or batch files that you want to run when GUI mode stage of Setup is complete. Note that all commands must be enclosed in quotation marks. Also, if you are using the command line (Cmd.exe) to run commands, programs, scripts, or batch files, then you need to use the /c parameter with the **cmd** command. For example, to create a new folder named Test on drive C, you type:

```
"cmd /c mkdir c:\Test"
```

To use Cmdlines.txt, you need to:

- Add the following section, entry, and value to your answer file:

```
[Unattended]

OemPreinstall = Yes
```

- Configure your Cmdlines.txt file, and save it in the \$OEM\$ folder in your distribution share.
- Copy all of the programs, scripts, and batch files that are listed in your Cmdlines.txt file to the \$OEM\$ folder in your distribution share.

For a worksheet to assist you in recording the commands, programs, scripts, and batch files that you want to run by using Cmdlines.txt, see “Answer File Settings Worksheet” (ACIUI\_5.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Answer File Settings Worksheet” on the Web at <http://www.microsoft.com/reskit>).

---

## Configuring [GuiRunOnce] to Perform Tasks

The [GuiRunOnce] section of an answer file contains a list of commands, programs, scripts, or batch files that run the first time a user logs on to the computer after the operating system is installed. You can configure [GuiRunOnce] to run multiple commands, programs, scripts, or batch files. The commands, programs, scripts, and batch files run synchronously, which means each command, program, script, or batch file runs to completion before the next one starts running. This lets you control the order in which tasks are performed.

The syntax for [GuiRunOnce] is:

```
[GuiRunOnce]

"command_1"

"command_2"

.

.

"command_x"
```

Where *command\_1*, *command\_2*, and *command\_x* refer to the commands, programs, scripts, or batch files that you want to run after the operating system is installed and a user logs on. Note that all commands must be enclosed in quotation marks.

To use [GuiRunOnce], you need to:

- Add the [GuiRunOnce] section and the corresponding commands to your answer file.
- Copy all of the programs, scripts, and batch files that are listed under [GuiRunOnce] to the \$OEM\$ folder in your distribution share.

For a worksheet to assist you in recording the commands, programs, scripts, and batch files that you want to run by using [GuiRunOnce], see “Answer File Settings Worksheet” (ACIUI\_5.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Answer File Settings Worksheet” on the Web at <http://www.microsoft.com/reskit>).

If you use the [GuiRunOnce] section to install software, you need to adhere to the following guidelines:

**You cannot run installation programs that require a restart**

You can automate installation tasks only if you can prevent the installation program from restarting the computer. When a computer restarts, all remaining entries in the [GuiRunOnce] section are lost. If the system restarts before completing entries listed in the [GuiRunOnce] section, the remaining items will not run. Therefore, you need to suppress restarts. If you cannot suppress a restart within the installation program, you can try to repack the application into a Windows Installer package. For more information about Windows Installer packaging, see the Windows Installer documentation link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

**You cannot run installation programs that rely on the Windows Explorer shell**

The Windows Explorer shell is not loaded when the operating system starts running commands, programs, scripts, or batch files that are listed in the [GuiRunOnce] section of an answer file. In some cases, you can get an updated installer program from the application vendor that does not rely on the Windows Explorer shell. If you cannot, you might be able to repack the application as a Windows Installer package (.msi file).

**You might need to run an installation program from a batch file so you can control the installation process with the /wait parameter**

Installation programs often start and stop several different processes. In some cases, when you are installing multiple applications, this can inadvertently cause the next installation program listed in the [GuiRunOnce] section to start before the previous installation program is finished running. When this occurs, the second installation program usually fails. To prevent this, you can run the installation programs from batch files by using the **start** command with the **/wait** parameter. This forces each installation program to run to completion before the next command listed in [GuiRunOnce] runs. For more information about using the **start** command to run installation programs in batch files, in Help and Support Center for Windows Server 2003, under **Support Tasks**, click **Tools**, click “Command-line reference A-Z”, and then click **Start**.

## Designing Setup Settings

An unattended installation relies on one of two Setup programs: a 16-bit Setup program called Winnt.exe, or a 32-bit Setup program called Winnt32.exe. You can run Winnt.exe on a computer that is running MS-DOS, Windows 3.1, or Windows for Workgroups. You can run Winnt32.exe on a computer that is running Windows 95, Windows 98, Windows Millennium Edition, Windows NT, Windows 2000, Windows XP, and the Windows Server 2003 family. Winnt.exe and Winnt32.exe can be found on a Windows XP Professional or Windows Server 2003 product CD. For a worksheet to assist you in recording Setup options for each of your unattended installations, see “Unattended Installation Worksheet” (ACIUI\_1.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Unattended Installation Worksheet” on the Web at <http://www.microsoft.com/reskit>).

---

### Choosing Winnt.exe Parameters

You can start Setup by using the Winnt.exe command line tool from MS-DOS, Windows for Workgroups, or Windows 3.1. Winnt.exe has the following syntax:

```
winnt [/s:[sourcepath]] [/t:[tempdrive]] [/u:[answer_file]] [/udf:id [,UDB_file]]  
[/r:folder] [/rx:folder] [/e:command] [/a]
```

Use the following parameter descriptions to determine which parameters to use for your unattended installation. For a worksheet to assist you in recording these parameters, see “Unattended Installation Worksheet” (ACIUI\_1.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Unattended Installation Worksheet” on the Web at <http://www.microsoft.com/reskit>).

#### **/s**

Specifies the source location of the Windows operating system files. The location must be a full path of the form *drive\_letter:\path\_to\_folder* or *\\server\path\_to\_shared\_folder*. The default is the current folder. Use this parameter if you are using a distribution share.

#### **/t**

Directs Setup to place temporary files on the specified drive and to install Windows on that drive. If you do not specify a location, Setup attempts to locate a drive for you.

#### **/u**

Performs an unattended installation with an answer file. The answer file provides answers to some or all of the prompts that the end user normally responds to during setup. If you use **/u**, you must also use **/s**.

#### **/udf**

Indicates an identifier (*id*) that Setup uses to specify how a uniqueness database file (.udf) modifies an answer file (see **/u**). The .udf file overrides values in the answer file, and the identifier determines which values in the .udf file are used. If no .udf file is specified, Setup prompts the user to insert a disk that contains the .udf file.



**/r**

Specifies an optional folder to create during setup. For example, you might create a folder named Drivers on the C drive, and then copy device driver files to the folder after the installation completes. The folder remains after Setup finishes.

**/rx**

Specifies an optional folder to create and to copy the contents of another folder to during setup. The folder is deleted after the Setup program stops running. For example, you might create a folder named Scripts on the C drive, and then copy scripts that you want to run during the installation to that folder. After the installation completes, the scripts and the folder are deleted.

**/e**

This parameter specifies a command to run after the GUI mode stage of Setup.

**/a**

This parameter enables accessibility options.

You cannot use Winnt.exe to perform an upgrade. You can perform only clean installations when you use Winnt.exe. In addition, you must use the 8.3 naming convention to name all of the files and folders in your distribution share. To adhere to the 8.3 naming convention, you cannot have more than 8 characters before the decimal point, and you must have a three-character extension after the decimal point. You need to use a \$\$Rename.txt file to convert 8.3 file names to long file names during setup. For more information about renaming files and folders during setup, see “Designing a Distribution Share” earlier in this chapter.

For more information about Winnt.exe parameters, see “Winnt.exe Command Line Options” in the *Microsoft Windows Corporate Deployment Tools User’s Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.

---

## Choosing Winnt32.exe Parameters

You can start Setup by using the Winnt32.exe command line tool from Windows 95, Windows 98, Windows Millennium Edition, Windows NT 4.0, Windows 2000, Windows XP Professional, and the Windows Server 2003 family. You cannot run Winnt32.exe on an Itanium-based computer from the extensible firmware interface (EFI), and no Winnt32.efi is available.

Winnt32.exe has the following syntax:

```
winnt32 [/checkupgradeonly] [/cmd:command_line] [/cmdcons]
[/copydir:{i386|ia64}\folder_name] [/copysource:folder_name]
[/debug[level]:[filename]] [/dudisable] [/dupprepare:pathname] [/dushare:pathname]
[/emsport:{com1|com2|usebiossettings|off}] [/emsbaudrate:baudrate]
[/m:folder_name] [/makelocalsource] [/noreboot] [/s:sourcepath]
[/syspart:drive_letter:] [/tempdrive:drive_letter:] [/udf:id [,UDB_file]]
[/unattend[num]:[answer_file]]
```

Use the following parameter descriptions to determine which parameters to use for your unattended installation. For a worksheet to assist you in recording these parameters, see “Unattended Installation Worksheet” (ACIUI\_1.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Unattended Installation Worksheet” on the Web at <http://www.microsoft.com/reskit>).

**/checkupgradeonly**

Checks your computer for upgrade and installation compatibility with Windows XP Professional and Windows Server 2003.

If you use this option with **/unattend**, no user input is required. Otherwise, the results are displayed, and you can save them with a specified file name. The default file name is Upgrade.txt in the systemroot folder.

**/cmd**

Instructs Setup to execute a specific command before beginning the final stage of the setup process. This occurs after your computer has restarted and after the Setup program has collected the necessary configuration information, but before the setup process finishes.

**/cmdcons**

Installs the Recovery Console as a startup option on a functioning x86-based computer. The Recovery Console is a command-line interface from which you can perform tasks such as starting and stopping services and accessing the local drive (including drives formatted with NTFS). You can use the Recovery Console only after Setup finishes.

**/copydir**

Creates one or more folders in the folder where the Windows files are installed.

**/copysource**

Creates one or more temporary folders in the folder where the Windows files are installed.

**/debug**

Creates a debug log at the level specified, for example, **/debug4:Debug.log**. The default log file is %SYSTEMROOT%\Winnt32.log, and the default debug level is 2. The log levels are: 0, representing severe errors; 1, representing errors; 2, representing warnings; 3 representing information; and 4, representing detailed information for debugging. Each level includes the levels under it.

**/dudisable**

Prevents Dynamic Update from running. Without Dynamic Update, Setup runs only with the original Setup files. This option disables Dynamic Update even if you set DUDisable equal to No in the [Unattended] section of your answer file.

**/dupprepare**

Prepares a distribution share so that it can be used with Dynamic Update files downloaded from the Windows Update Web site. This distribution share can then be used for installing Windows for multiple clients.

**/dushare**

Specifies a distribution share on which you previously downloaded Dynamic Update files (updated files for use with Setup) from the Windows Update Web site, and on which you previously ran **/dupprepare:pathname**. When run on a client, specifies that the client installation uses the updated files on the distribution share specified in *pathname*.

**/emsport**

Enables or disables Emergency Management Services during setup and after a member of the Windows Server 2003 family of operating systems has been installed. With Emergency Management Services, you can remotely manage a server in emergency situations that normally require a local keyboard, mouse, and monitor, such as when the network is unavailable or the server does not function properly. Emergency Management Services has specific hardware requirements, and is available only for products in the Windows Server 2003 family. For more information about Emergency Management Services, see “Planning for Remote Server Management” in *Planning Server Deployments* of this kit.

**/emsbaudrate**

For x86-based computers, this parameter specifies the baud rate for Emergency Management Services. (The option is not applicable for Itanium-based computers.) Must be used with **/emsport:com1** or **/emsport:com2** or else **/emsbaudrate** is ignored.

**/m**

Specifies that Setup copies replacement files from an alternative location. Instructs Setup to look in the alternative location first, and, if files are present, to use them instead of the files from the default location.

**/makelocalsource**

Instructs Setup to copy all installation source files to your local hard disk. Use **/makelocalsource** when installing from a CD to provide installation files when the CD is not available later in the installation.

**/noreboot**

Instructs Setup not to restart the computer after the file-copy stage of Setup finishes, so that you can execute another command.

**/s**

Specifies the location of the Windows files. To simultaneously copy files from multiple servers, type the */s:sourcepath* option multiple times (up to a maximum of eight).

**/syspart**

On an x86-based computer, this parameter specifies that you can copy Setup startup files to a hard disk, mark the disk as active, and then install the disk onto another computer. When you start the computer onto which you have installed the disk, it automatically starts with the next phase of Setup. You must always use the **/tempdrive** parameter with the **/syspart** parameter.

You can start Winnt32.exe with the **/syspart** option on an x86-based computer running Windows NT 4.0, Windows 2000, or Windows XP Professional. The computer cannot be running Windows 95, Windows 98, or Windows Millennium Edition.

**/tempdrive**

Directs Setup to place temporary files on the specified partition. For a new installation, Windows is installed on the specified partition. For an upgrade, the **/tempdrive** option affects the placement of temporary files only; the operating system is upgraded in the partition from which you run Winnt32.exe.

**/udf**

Indicates an identifier (*id*) that Setup uses to specify how a uniqueness database file (.udf) modifies an answer file (see the **/unattend** option).

If you start from the Windows Server 2003 operating system CD and run an unattended setup, you cannot use the **/udf** command-line option for Winnt32.exe.

**/unattend**

Upgrades your previous version of Windows 98, Windows Millennium Edition, Windows NT 4.0, or Windows 2000 in unattended mode (without user input). Setup downloads the Dynamic Update files from Windows Update and includes these files in the installation. All user settings are taken from the previous installation, so no user intervention is required during setup.

**/unattend[num]:[answer\_file]**

Performs a fresh installation of Windows in unattended mode using the specified answer file. Setup downloads the Dynamic Update files from the Windows Update Web site and includes these files in the installation. The specified *answer\_file* provides Setup with your custom specifications.

For more information about Winnt32.exe parameters, see “Winnt32.exe Command Line Options” in the *Microsoft Windows Corporate Deployment Tools User’s Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.

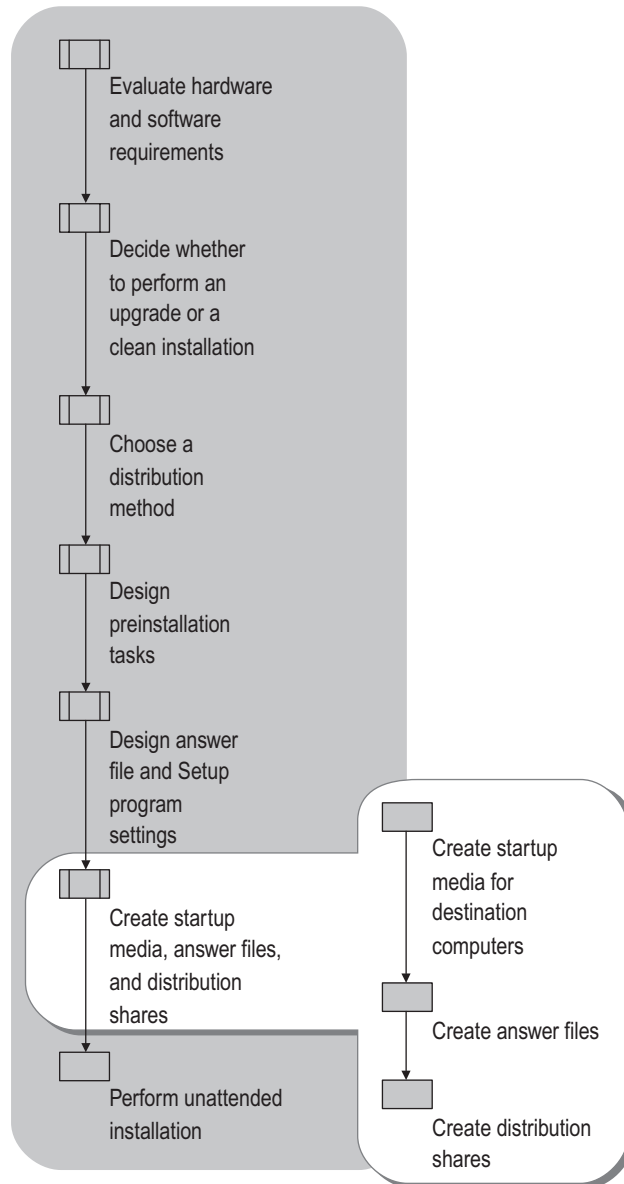
---

## Creating Startup Media, Answer Files, and Distribution Shares

After you design your unattended installation, you need to implement your design. Usually, your deployment team is responsible for implementing your design decisions. The worksheets that are referenced in this chapter contain sufficient design information for your deployment team to perform these tasks.

Figure 2.8 shows the steps you must follow to create startup media, answer files, and distribution shares for an unattended installation.

**Figure 2.8 Creating Startup Media, Answer Files, and Distribution Shares**



## Creating Startup Media for Destination Computers

If you are performing clean installations, and you want to configure the hard disks on your destination computers, you might need to create startup media to start the destination computer. This section provides guidelines for choosing and creating appropriate startup media.

If you are performing upgrades, you can skip this section because you cannot use startup media to start destination computers. You must start the destination computers by using the operating system that is installed on those computers.

Likewise, if you are performing clean installations on destination computers that are running Windows 95, Windows 98, Windows Millennium Edition, Windows NT 4.0, Windows 2000, or Windows XP Professional, and you do not want to configure hard disks on your destination computers, then you do not need to create startup media. You can perform an unattended installation by starting the destination computers with the operating system that is already installed on those computers.

---

### Choosing Startup Media

Choosing startup media is a two-step process. First, you determine what type of startup media your hardware supports. Not every organization can support CD or DVD startup media. Next, you determine whether one particular type of startup media is more appropriate than another, based on the way you are performing your unattended installations.

### Evaluating Hardware Support for Startup Media

Follow these steps to determine which type of startup media your organization can support.

1. Evaluate your hardware inventory for floppy disk support.

To use a floppy disk as startup media, every destination computer must have a floppy drive, and the boot-order sequence in every BIOS must list the floppy drive.

2. Evaluate your hardware inventory for CD or DVD support.

To use a CD or DVD as startup media, all of your destination computers must have bootable CD or DVD drives. Some older CD drives and many DVD drives are not bootable devices. In addition, the boot-order sequence in the BIOS of each computer must include the CD or DVD drive. Some older BIOSes do not let you add the CD or DVD drive to the boot-order sequence.

3. Evaluate your CD or DVD writeable device.

To create your own CD or DVD startup media, you must have the proper hardware, software, and instructions to create bootable CDs or DVDs. Microsoft does not provide tools for creating CD or DVD startup media; however, several manufacturers provide the hardware, software, and system files that you need to create bootable CDs or DVDs.

If your organization supports only floppy disk startup media, you are ready to create your startup media. For more information about creating startup media, see “Creating Startup Media” later in this chapter.

## Choosing Startup Media

If you have the proper hardware and software to create CD or DVD startup media, and the destination computers in your organization support CD or DVD startup media, you need to determine which type of startup media is most suitable for your unattended installation.

Use a floppy disk to start your destination computers if:

- Your design requirements allow you to use Winnt.exe to start Windows Setup. Winnt.exe runs only under MS-DOS, and has limited functionality compared to Winnt32.exe. For more information about Winnt.exe and Winnt32.exe, see “Performing Unattended Installations” later in this chapter, and the *Microsoft Windows Corporate Deployment Tools User’s Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.
- You want to create partitions or format disks before you install the operating system onto the destination computer, and your disk configuration tools can run under MS-DOS.
- You do not want to use Dynamic Update to download and install critical updates and device drivers from the Internet. You can use Dynamic Update to download and install critical updates and device drivers from a server within your organization, but only if you start your destination computers with a floppy disk that provides network support.

Use a CD or DVD to start your destination computers if:

- Your design requires Winnt32.exe to start Windows Setup. Winnt32.exe is a 32-bit program that has greater functionality than Winnt.exe. However, Winnt32.exe can be used only if you start a destination computer with the operating system CD; or with Windows 95, Windows 98, Windows Millennium Edition, Windows NT 4.0, Windows 2000 (32-bit edition), Windows XP Professional (32-bit edition), or Windows Server 2003 (32-bit edition). You cannot run Winnt32.exe on a destination computer that is running Windows Advanced Server, Limited Edition (64-bit edition). For more information about Winnt.exe and Winnt32.exe, see “Performing Unattended Installations” later in this chapter and the *Microsoft Windows Corporate Deployment Tools User’s Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.
- You want to create partitions or format disks before you install the operating system onto your destination computer, and your disk configuration tools can run under a 32-bit operating system.

## Creating Startup Media

Startup media contains the system files and device drivers that are necessary to start a computer so that the primary hard disk is accessible, but not in use. Startup media might also contain network adapter and network drivers, CD and DVD device drivers, disk configuration tools, and scripts or batch files. The startup media that you choose to use depends mostly on personal preference and your organization's capabilities; however, your startup media must:

- Provide network support if you need to access a distribution share that is on a shared folder on the network, or if you need to access Dynamic Update files on a shared folder on the network.
- Provide CD or DVD device support if you need to access a distribution share on a CD or DVD, or if you need to access disk configuration tools on a CD or DVD.
- Support any tools you need to configure disks before you perform your unattended installation.
- Be able to run the Setup program that your design requires — that is, either Winnt.exe or Winnt32.exe.

You can use the following methods to create startup media:

**Create a TCP/IP boot disk** You can use a Windows NT Server 4.0 operating system CD to create startup media if you need network support. You must create a separate disk for each network adapter. For more information, see the TCP/IP Boot Disk link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

**Create a network boot disk by using Windows 2000** You can use the Network Client Administrator and a computer running Windows 2000 to create startup media if you need network support. You must have a Windows NT Server 4.0 operating system CD. For more information, see article Q252448, "How to Create an MS-DOS Network Startup Disk in Windows 2000" 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>.

**Create a network boot disk by adding NDIS drivers to an MS-DOS boot disk** You can use this method if you need network support. You must create a separate disk for each network adapter. You must have an MS-DOS boot disk that was created by using the Network Client Administrator, which is included in the \Clients folder on the Windows NT Server 4.0 operating system CD. For more information, see articles Q142857, "How to Create a Network Installation Boot Disk," and Q128800, "How to Provide Additional NDIS2 Drivers for Network Client 3.0," in the Microsoft Knowledge Base. To find these articles, see the Microsoft Knowledge Base link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.



**Create an MS-DOS boot disk** If you are running Windows XP Professional or Windows Server 2003, you can create an MS-DOS boot disk by using the following procedure: In Windows Explorer, right-click a floppy drive, click **Format** on the shortcut menu, and then select the **Create an MS-DOS startup disk** check box.

**Create a bootable CD or DVD** You can use your writable CD or DVD device to create bootable CDs or DVDs. For more information about creating bootable CDs or DVDs, see the documentation that came with your CD or DVD drive or the documentation for the software that you use to create CDs or DVDs.

---

## Creating Answer Files

An answer file contains the operating system settings that you want to configure during an unattended installation. Before you create an answer file, you need to design your answer file settings. For a worksheet to assist you in recording the settings, see “Answer File Settings Worksheet” (ACIUI\_5.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Answer File Settings Worksheet” on the Web at <http://www.microsoft.com/reskit>).

There are two ways to create an answer file:

- You can use Setup Manager (Setupmgr.exe) to create a minimal answer file that contains critical sections and entries necessary for an unattended installation. Setup Manager is an interactive tool that prompts you for configuration settings, and then builds an answer file based on your responses.
- You can use a text editor, such as Notepad, to manually build an answer file by adding sections and entries to a text file. Using a text editor to build an answer file is often faster and easier than using Setup Manager; however, text editors are more error prone because they do not check answer file syntax.

Typically, you use Setup Manager to build a new answer file, and then use Notepad to manually configure the answer file. You can use the “Answer File Settings Worksheet” (ACIUI\_5.doc) to help you configure your answer file.

## Creating an Answer File with Setup Manager

You can use Setup Manager to create an answer file, and configure a limited number of answer file settings. Setup Manager is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD. You can run Setup Manager only on Windows XP Professional or on Windows Server 2003.

### ► To create an answer file by installing and running Setup Manager

1. From the Deploy.cab file in the \Support\Tools folder of the Windows Server 2003 operating system CD, copy the Setupmgr.exe file to your hard disk.
2. At the command prompt, use the **cd** command to change your current folder to the folder that contains Setupmgr.exe, type **setupmgr**, and then press Enter.
3. Follow the instructions that appear on your screen.

Setup Manager prompts you for the configuration settings listed in Table 2.5. To configure other settings, you must manually edit the answer file as a text file.

**Table 2.5 Answer File Settings That Can Be Configured with Setup Manager**

Setup Manager Page	Answer File	Section	Entry
User Interaction Page	Unattend.txt	[Unattended]	UnattendMode
Name and Organization Page	Unattend.txt	[UserData]	FullName OrgName
Display Settings Page	Unattend.txt	[Display]	BitsPerPel XResolution YResolution VRefresh
Time Zone Page	Unattend.txt	[GuiUnattended]	TimeZone
Product Key Page	Unattend.txt	[UserData]	ProductKey
Computer Names Page	Unattend.txt	[UserData]	ComputerName
Administrator Password Page	Unattend.txt	[GuiUnattended]	AdminPassword* EncryptedAdminPassword
Networking Computers Page	Unattend.txt	[Networking] [NetAdapters] [NetClients] [NetProtocols]	
Workgroup or Domain Page	Unattend.txt	[Identification]	

(continued)

**Table 2.5 Answer File Settings That Can Be Configured with Setup Manager (continued)**

Setup Manager Page	Answer File	Section	Entry
Windows Components Page	Unattend.txt	[Components]	
Telephony Page	Unattend.txt	[TapiLocation]	
Regional Settings Page	Unattend.txt	[RegionalSettings]	
Languages Page	Unattend.txt	[RegionalSettings]	Language
Browser and Shell Settings Page	Unattend.txt	[FavoritesEx]	
Installation Folder Page	Unattend.txt	[Unattended]	TargetPath
Install Printers Page	Unattend.txt	[GuiRunOnce]	
Run Once Page	Unattend.txt	[GuiRunOnce]	
Additional Commands Page	Cmdlines.txt	[Commands]	

\* The value for AdminPassword cannot begin with an asterisk (\*). Using a password that begins with an asterisk can cause the password to be set to a null value.

For more information about Setup Manager, see “Using Setup Manager” and “Setup Manager Settings” in the *Microsoft Windows Corporate Deployment Tools User’s Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.

## Creating an Answer File Manually

You can create or modify an answer file manually by using a text editor, such as Notepad. If you created an answer file by using Setup Manager, the answer file already has several sections and entries. You can add more sections and entries by simply typing the section, entry, and value. However, you can use only valid sections, entries, and values. You cannot create sections, entries or values that are not listed in the “Answer File Settings Worksheet” (ACIUI\_5.doc).

Use the following guidelines when you manually create or modify an answer file:

- Sections are always enclosed in square brackets (for example, [Unattended]).
- Sections and entries are not case sensitive.
- Entries must have valid values. For example, “on” is not equivalent to “enable,” and “off” is not equivalent to “disable.” Invalid sections and entries can generate errors, or cause Setup to fail.
- Each entry must have a value.

In addition, you do not need to add every section or entry to the answer file. Setup ignores missing sections and entries.

## Creating Distribution Shares

To install Windows XP Professional or Windows Server 2003 on multiple computers over a network, you must create at least one set of distribution shares. The distribution shares typically reside on a server to which each of your destination computers can connect. You can use the same set of distribution shares with different answer files to create different system configurations. Even if you intend to use disk imaging as your installation method, building your master installations with distribution shares provides consistent implementations for a variety of system types. In addition, you can use distribution shares to update future images by editing the files in the distribution shares or by modifying the answer files to generate updated images without having to rebuild each of your master computers.

Before you can create your distribution shares, you need to design them. For a worksheet to assist you in recording the design requirements, see “Distribution Share Worksheet” (ACIUI\_2.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Distribution Share Worksheet” on the Web at <http://www.microsoft.com/reskit>). You can then use the Distribution Share Worksheet to help you create your distribution shares.

There are two ways to create a distribution share:

- You can use Setup Manager to create a minimal distribution share that contains the system files and device drivers necessary for an unattended installation. Setup Manager is an interactive tool that prompts you for configuration settings, and then builds a distribution share based on your responses.
- You can manually copy files and folders to a distribution share. However, this method is vulnerable to mistakes, and it is recommended that you use it to make only minor changes to your distribution shares.

Typically, you use Setup Manager to create your basic distribution shares. Then, you manually add files and folders to the distribution shares based on your design requirements.



### **To create a distribution share by installing and running Setup Manager**

1. From the Deploy.cab file in the \Support\Tools folder of the operating system CD, copy the Setupmgr.exe file to your hard disk.
2. At the command prompt, use the **cd** command to change your current folder to the folder that contains Setupmgr.exe, type **setupmgr**, and then press Enter.
3. Follow the instructions that appear on your screen.

Use the following procedure to manually create a distribution share.

► **To manually create a distribution share**

1. Create a shared folder on a server and give it a name that describes the operating system you are installing. For example, if you are creating a distribution share for Windows XP Professional installations, you might name the folder XP\_Pro. Be sure each of your destination computers can connect to the shared folder. This folder is your distribution share.
2. Set permissions on the shared folder so that only authorized users can access the folder.  
Authorized users are those users who perform unattended installations in your organization.
3. Copy the contents of the i386 folder on your operating system CD to the i386 folder on your server.
4. In the shared folder, create a folder named \$OEM\$.  
The \$OEM\$ folder is the top level folder for all supplemental installation files — such as device drivers, utilities, programs, and scripts — that you want copied to you destination computers.
5. Copy all supplemental files to the \$OEM\$ folder.  
Be sure to follow the structure shown in Figure 2.5. You can also use your “Distribution Share Worksheet” (ACIUI\_2.doc) to help you identify the structure and contents of the \$OEM\$ folder.

---

## Performing Unattended Installations

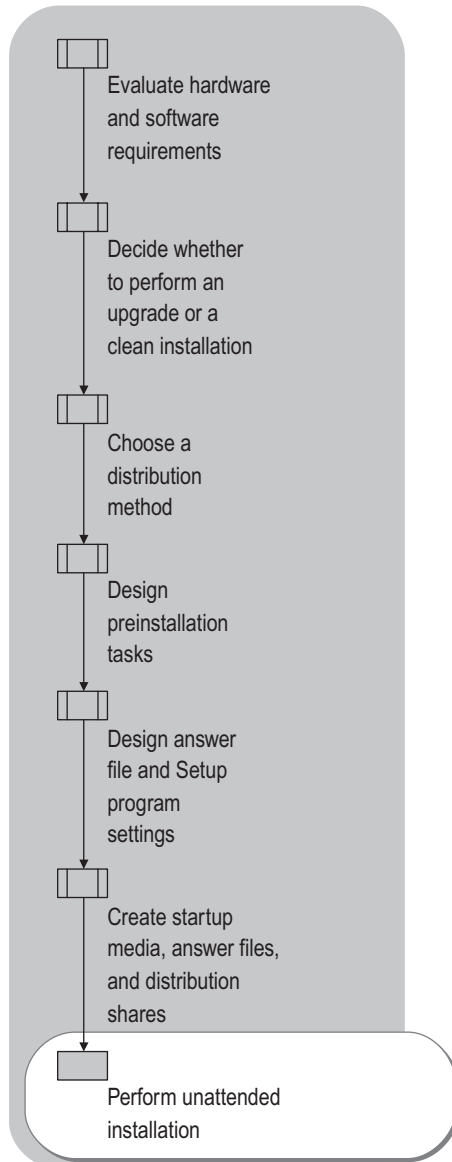
There are several ways to perform an unattended installation:

- You can start a destination computer with the operating system CD, and use a Winnt.sif answer file to automate a clean installation of the operating system.
- You can start a destination computer with an MS-DOS startup disk, and then run Winnt.exe with an answer file to perform an automated clean installation.
- You can start a destination computer with a 32-bit operating system — for example, Windows 95, Windows 98, Windows Millennium Edition, Windows NT 4.0, Windows 2000, Windows XP Professional, or Windows Server 2003 — and then run Winnt32.exe with an answer file to perform an automated clean installation.
- You can start a destination computer with a 32-bit operating system — for example, Windows 95, Windows 98, Windows Millennium Edition, Windows NT 4.0, Windows 2000, Windows XP Professional, or Windows Server 2003 — and then run Winnt32.exe with an answer file to perform an automated upgrade.

To determine which unattended installation method to use, use the information you recorded in the “Unattended Installation Worksheet” (ACIUI\_1.doc). This worksheet contains your overall design requirements, such as upgrade and clean installation requirements, startup method, and distribution requirements.

Figure 2.9 shows when you perform an unattended installation.

**Figure 2.9 Performing Unattended Installations**



## Performing a Clean Unattended Installation with an Operating System CD

Before you perform an unattended installation with an operating system CD, verify that:

- Your answer file is named Winnt.sif, and that it is saved on a floppy disk.
- The BIOS settings in your destination computer list the CD-ROM drive as the first startup device.
- Your answer file contains the following entries, which are required if you perform an unattended installation with an operating system CD:

```
[Data]
```

```
MsDosInitiated=0
```

```
UnattendedInstall=Yes
```

```
[Unattended]
```

```
OemPreinstall=No
```

```
UnattendSwitch=Yes
```

- Make sure the destination computer is connected to the network (if necessary), and that all peripheral devices, such as printers, scanners, and cameras, are connected to the computer.

After you perform these verification steps, you are ready to perform the unattended installation.

### ► To perform an unattended installation with an operating system CD

1. Perform the user state migration tasks that are discussed in your user state migration plan (if you have one).
2. Insert the Windows XP Professional or Windows Server 2003 operating system CD into the CD-ROM drive of the destination computer.
3. Start the destination computer.
4. Press any key when you see “**Press any key to boot from the CD**” appear on your screen. This message appears during text mode stage of Setup. This message does not appear in a dialog box.
5. Insert the floppy disk containing the Winnt.sif file into the floppy disk drive of the destination computer.

After you complete this procedure, Setup starts, reads the Winnt.sif answer file, and installs the operating system with the configuration settings specified in your answer file.

## Performing a Clean Unattended Installation with an MS-DOS Startup Disk

Before you perform an unattended installation with an MS-DOS startup disk, verify that:

- The destination computer is connected to the network if you are using a distribution share, and any peripheral devices, such as scanners, printers, and cameras, are connected to the destination computer.
- Your MS-DOS startup disk contains the appropriate device drivers for network connectivity, DVD drives, and any other peripherals that your unattended installation requires. For example, if you are installing from a distribution share on a server, the destination computer needs network connectivity. Likewise, if you are installing from the operating system CD, the destination computer needs to load the drivers for the DVD drive.
- The BIOS settings in your destination computer list the floppy disk drive as the first or second startup device.
- You have the proper permissions to access the distribution share, if you are installing from a distribution share.
- Your answer file is saved on the MS-DOS startup disk or in your distribution share.

After you perform these verification steps, you are ready to perform the unattended installation.

### ► **To perform an unattended installation with an MS-DOS startup disk**

1. Perform the tasks described in your user state migration plan (if you have one).
2. Perform the tasks described in your disk configuration plan (if you have one).
3. Insert the MS-DOS startup disk into the floppy disk drive, and make sure you do not have a CD in the CD-ROM drive.
4. Start the destination computer.
5. If you are installing from a distribution share that is on a CD, or if you are installing from an operating system CD, insert the CD into the CD-ROM drive.
6. At the command prompt, run Winnt.exe with the parameters listed on the “Unattended Installation Worksheet (ACIUI\_1.doc).

After you complete this procedure, Setup starts, reads your answer file, and installs the operating system with the configuration settings specified in your answer file.



## Performing a Clean Unattended Installation with a 32-bit Operating System

Before you perform an unattended installation with a 32-bit operating system, verify that:

- The destination computer is connected to the network, and that you have the proper permissions to access your distribution share if you are installing from a distribution share.
- Your answer file is saved on a floppy disk or in your distribution share.
- You have the proper permissions to access the distribution share, if you are installing from a distribution share.

After you perform these verification steps, you are ready to perform the unattended installation.



### **To perform a clean unattended installation with a 32-bit operating system**

1. Perform the tasks described in your user state migration plan (if you have one).
2. Perform the tasks described in your disk configuration plan (if you have one).
3. Start the destination computer.
4. If you are installing from a distribution share that is on a CD, or if you are installing from an operating system CD, insert the CD into the CD-ROM drive.
5. At the command prompt, run Winnt32.exe with the parameters listed on the “Unattended Installation Worksheet (ACIUI\_1.doc).

After you complete this procedure, Setup starts, reads your answer file, and installs the operating system with the configuration settings specified in your answer file.

## Performing an Unattended Upgrade Installation

Before you perform an upgrade unattended installation, verify that:

- Your answer file is saved on a floppy disk.
- You have the product CD for the operating system you are installing.
- If you are upgrading from Windows 98 or Windows Millennium Edition to Windows XP Professional, you have the following entries in your answer file:

```
[Unattended]
```

```
Win9xUpgrade=Yes
```

- If you are upgrading a server to Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; or Windows Server 2003, Web Edition, you have the following entries in your answer file:

```
[Unattended]
```

```
NtUpgrade=Yes
```

- You do not have the following entries in your answer file. These entries cannot be used if you are performing an upgrade unattended installation:

```
[Unattended]
```

```
OemPreinstall=Yes
```



### Note

Setup only reads the following entries in an answer file during an unattended upgrade installation: Win9xUpgrade, NtUpgrade, OemPreinstall, ProductKey, AutoActivate, DuDisable, DuShare, and DuStopOnError.

After you perform these verification steps, you are ready to perform the unattended installation.



### To perform an unattended upgrade installation

1. Perform the tasks described in your user state migration plan (if you have one).
2. Start the destination computer.
3. Insert the floppy disk containing your answer file into the floppy drive.
4. Insert the product CD into the CD-ROM drive.
5. At the command prompt, run Winnt32.exe with the parameters listed on the “Unattended Installation Worksheet (ACIUI\_1.doc).

After you complete this procedure, Setup starts, reads your answer file, and installs the operating system with the configuration settings specified in your answer file.

# Additional Resources

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

## Related Information

- “Choosing an Automated Installation Method” in this book for more information about planning Sysprep installations.
- “Designing Image-based Installations with Sysprep” in this book for more information about answer files, distribution shares, and unattended and automated installations.
- “Migrating User State” in this book for more information about migrating user data and settings.
- “Designing a Group Policy Infrastructure” in *Designing a Managed Environment* of this kit for more information about folder redirection.
- “Planning for Remote Server Management” in *Planning Server Deployments* of this kit for more information about Emergency Management Services.
- The *Server Management Guide* of the *Windows Server 2003 Resource Kit* (or see the *Server Management Guide* on the Web at <http://www.microsoft.com/reskit>) for more information about disk partitions and file systems.
- *Microsoft Windows Corporate Deployment Tools User’s Guide* (Deploy.chm) for more information about using Sysprep. Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.
- The Windows Catalog link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.
- The Windows Update link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.
- The Windows Preinstallation Environment link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources> for information about Windows PE and Windows PE licensing plans.
- The Microsoft Platform SDK link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources> to download the Core SDK which contains information about configuring a .theme file.
- The TCP/IP Boot Disk link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources> for more information about creating a TCP/IP boot disk for distributing disk images across a network.

- The Microsoft TechNet articles “User State Migration in Windows XP,” “Step-by-Step Guide to Migrating Files and Settings,” “Deploying Windows XP Part I: Planning,” and “Deploying Windows XP Part II: Implementing” for more information about migrating user data and settings.
- Article Q294895, “Description of the Application Compatibility Toolkit 2.0 for Windows XP,” in the Microsoft Knowledge Base.
- Article Q216573, “How Windows Determines ACPI Compatibility,” and article Q298898, “How to Determine the Hardware Abstraction Layer (HAL) That Is Used in Windows XP,” in the Microsoft Knowledge Base for more information about determining the type of HAL that is installed on a computer.
- Article Q252448, “How to Create an MS-DOS Network Startup Disk in Windows 2000,” in the Microsoft Knowledge Base for more information about creating a network boot disk by using a Windows NT Server 4.0 operating system CD.
- Article Q167685, “How to Create an El Torito Bootable CD-ROM,” in the Microsoft Knowledge Base for more information about using the El Torito specification to create a bootable CD.
- Articles Q142857, “How to Create a Network Installation Boot Disk,” and Q128800, “How to Provide Additional NDIS2 Drivers for Network Client 3.0,” in the Microsoft Knowledge Base for more information about creating a network boot disk by adding NDIS and NDIS2 drivers to an MS-DOS boot disk.

### **Related Tools**

- **Upgrade Advisor**

Use Upgrade Advisor to identify incompatible software and hardware on a destination computer before you perform a clean installation or an upgrade. To download the Upgrade Advisor tools, see the Windows Upgrade Advisor link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>. You also can run the Upgrade Advisor tools by using the **/checkupgradeonly** parameter with the Winnt32.exe tool. The Winnt32.exe tool is included in the i386 folder on the Windows XP Professional operating system CD and on the Windows Server 2003 operating system CD.
- **User State Migration Tool**

Use the User State Migration tool to save user settings and data before you perform an unattended installation. To download a free version of the User State Migration Tool, see the User State Migration Tool link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.
- **Microsoft Baseline Security Analyzer**

Use the Microsoft Baseline Security Analyzer to identify security vulnerabilities that require further configuration after you perform an unattended installation. See article Q320454, “Microsoft Baseline Security Analyzer (MBSA) Version 1.0 Is Available” 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>.

### 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.

- “Using roaming user profiles” in Help and Support Center for Windows Server 2003, for more information about roaming profiles
- “Disk Management overview” in Help and Support Center for Windows Server 2003, for more information about configuring disks.
- “Best practices for permissions and user rights” in Help and Support Center for Windows Server 2003, for more information about permissions.
- “Start” in Help and Support Center for Windows Server 2003, for more information about using the **start** command to run installation programs in batch files. To find “Start” in Help and Support Center for Windows Server 2003, look under **Support Tasks**, click **Tools**, click **Command-line reference A-Z**, and then click **Start**.

### Related Job Aids

- “Unattended Installation Worksheet” (ACIUI\_1.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Unattended Installation Worksheet” on the Web at <http://www.microsoft.com/reskit>) for a worksheet to help you design your unattended installations.
- “Distribution Share Worksheet” (ACIUI\_2.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Distribution Share Worksheet” on the Web at <http://www.microsoft.com/reskit>) for a worksheet to help you record information about your distribution shares.
- “Renamed Files and Folders Worksheet” (ACIUI\_3.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Renamed Files and Folders Worksheet” on the Web at <http://www.microsoft.com/reskit>) for a worksheet to help you record information about your renamed files and folders.
- “Dynamic Update Worksheet” (ACIUI\_4.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Dynamic Update Worksheet” on the Web at <http://www.microsoft.com/reskit>) for a worksheet to help you record information about your Dynamic Update design.
- “Answer File Settings Worksheet” (ACIUI\_5.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Answer File Settings Worksheet” on the Web at <http://www.microsoft.com/reskit>) for a worksheet to help you record your answer file settings.



# Designing Image-based Installations with Sysprep



Use the System Preparation tool (Sysprep), included with the Microsoft® Windows® operating system, to perform image-based installations when you want to install identical operating systems and software configurations on multiple computers as quickly as possible. By carefully planning and designing your image-based installation, you can accommodate hardware and software differences among computers, minimize end-user interaction during installation, and reduce the number of images you have to manage.

**In This Chapter**

**Overview of Image-based Installations ..... 92**  
**Identifying Inventory Requirements for Image-based Installations..... 97**  
**Defining Disk Images..... 106**  
**Designing the Image Delivery Process..... 114**  
**Designing Preinstallation Tasks for Image-based Installations..... 121**  
**Designing Automated Setup Tasks ..... 126**  
**Creating Disk Images ..... 141**  
**Creating Startup Media for Destination Computers ..... 153**  
**Deploying Disk Images ..... 157**  
**Additional Resources..... 158**

**Related Information**

- For more information about planning Sysprep installations, see “Choosing an Automated Installation Method” in this book.
- For more information about unattended installations, see “Designing Unattended Installations” in this book.

# Overview of Image-based Installations

*Image-based installation* is a method of copying, or cloning, preconfigured operating systems and software applications onto clients and servers. You can perform image-based installations of the Microsoft® Windows® XP Professional operating system and the Microsoft® Windows® Server 2003, Standard Edition; Windows® Server 2003, Web Edition; and Windows® Server 2003, Enterprise Edition operating systems by using Sysprep and a third-party disk-imaging program.

Image-based installation is a suitable deployment method if you need to:

- Install identical operating systems and software configurations on multiple computers.
- Install an operating system and software configuration as quickly as possible.
- Perform clean installations of an operating system, rather than upgrade an existing installation.
- Minimize end-user interaction and post-installation tasks.
- Install operating systems on computers that have similar hardware and compatible hardware abstraction layer (HAL).

In addition to these deployment solutions, you can customize an image-based installation to accommodate different hardware and software requirements; this allows you to use one disk image to deploy several different hardware and software configurations.

As a deployment solution, image-based installation requires substantial up-front planning and design. This chapter is designed to help IT professionals in medium and large organizations plan and design an image-based installation using Sysprep and a third-party disk-imaging program. It is assumed that you have already designed the client and server configurations that you want to deploy in your organization. This includes designing the configuration of all networking, directory services, and security components. You will use this client and server design information throughout this chapter to customize your image-based installation.

This chapter does not discuss image-based installation from an operations standpoint. In other words, the planning process and design decisions that are discussed in this chapter apply only to corporate deployments and rollouts; they do not apply to ongoing operational tasks such as reinstallation after a hard disk crash or reinstallation due to software or hardware failure.



## Note

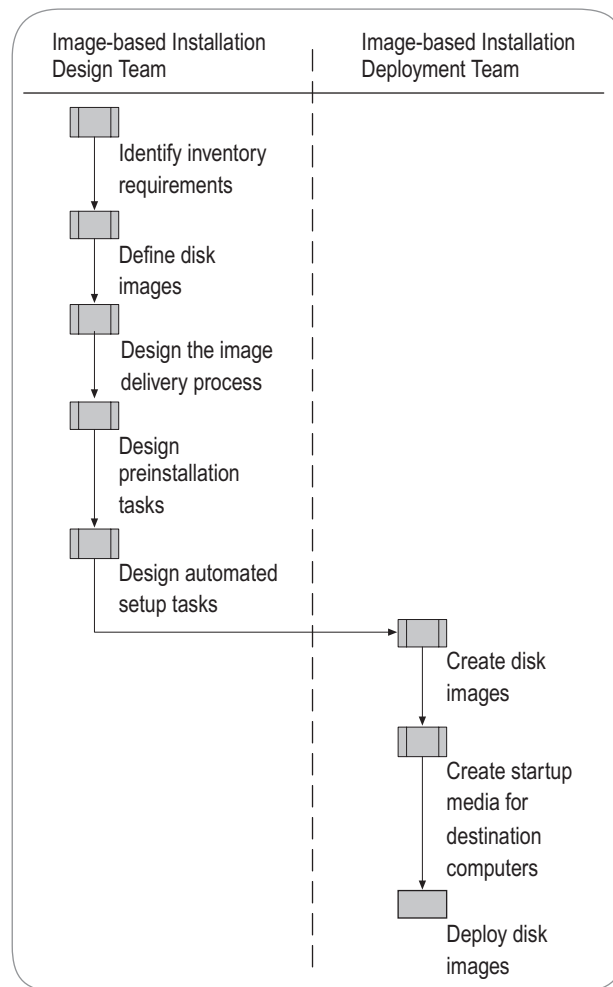
For a list of the job aids available to assist you in deploying image-based installations with Sysprep, see “Additional Resources” later in this chapter.



## Image-based Installation Design Process

Designing an image-based installation involves a design team and a deployment team. The design team is responsible for assessing your current environment to identify inventory requirements, defining disk image requirements, and designing the overall deployment process, including the image delivery process, preinstallation tasks, and automated setup tasks. The deployment team is responsible for implementing all design decisions, including creating disk images and startup media and deploying the disk images. Figure 3.1 shows the process for designing image-based installations.

**Figure 3.1 Designing Image-based Installations**



## Image-based Installation Background

To perform an image-based installation, you first set up a *master installation* — a computer with the operating system, software applications, and configuration settings that you want to install onto the destination computers in your organization. Then you run Sysprep, which prepares the master installation so that you can create a *disk image* (that is, a functionally identical replica of its disk) that can be copied onto multiple computers. Next, you use a third-party disk-imaging program to create the disk image of the master installation. Finally, you copy the disk image onto your destination computers.

You need two tools to perform an image-based installation: Sysprep, which can be found on any Windows XP Professional or Windows Server 2003 operating system CD; and a third-party disk-imaging program, which you must purchase from a third-party vendor. The Sysprep tool consists of three separate programs: Sysprep.exe, Setupcl.exe, and Factory.exe. However, you only run Sysprep.exe; Setupcl.exe and Factory.exe are secondary programs that Sysprep.exe runs as needed. To obtain Sysprep, open the Support\Tools folder on any Windows XP Professional or Windows Server 2003 operating system CD, and then open Deploy.cab. For more information about using Sysprep, see the *Microsoft® Windows Corporate Deployment Tools User's Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.

You run Sysprep on the master computer before you create an image of the master computer's hard disk. Sysprep configures various operating system settings on the master computer to ensure that every copy of the master computer's disk image is unique when you distribute it to a destination computer. Specifically, Sysprep configures a master installation so that unique security identifiers (SIDs) are generated on each destination computer. Sysprep also configures the master computer's disk image so that every destination computer starts in a special setup mode known as *Mini-Setup*. After you copy a disk image onto a destination computer, Mini-Setup runs the first time you start the destination computer.



### Note

You can run Sysprep from the command line or from the graphical user interface (GUI). When you run Sysprep from the command line, you can use various command-line parameters to control the way Sysprep runs. When you run Sysprep from the GUI, you use check boxes and command buttons to control the way Sysprep runs. This chapter assumes you are running Sysprep from the command line.

You use the third-party disk-imaging program to create an image of the master computer's hard disk. You also use the disk-imaging program to copy the disk image from the master computer onto a shared folder or a CD, and from the shared folder or CD onto a destination computer.

## Requirements for Image-based Installation

You can use image-based installation to deploy operating systems and software applications to desktop computers, portable computers, and servers. However, image-based installation is dependent on several factors and can be used only when certain conditions are met. The following are some of the key conditions.

**Clean installation only** You can only use image-based installation to install a clean version of the operating system and clean versions of software applications. You cannot use image-based installation to upgrade an operating system or software configuration.

**Limited server configuration** Some server components must be installed and configured after the image-based installation is complete. These include Certificate Services, Cluster service, and any software that is dependent on the Active Directory® directory service. These also include any application or service that stores the computer name or the computer SID and cannot recover if the computer name or SID changes.

**HAL compatibility** You can only perform an image-based installation if the HAL on the disk image is compatible with the hardware on the destination computer. In some cases, Windows XP Professional and Windows Server 2003 automatically upgrade the HAL that is on a disk image to suit the HAL requirements of a destination computer, but this can only occur if the HAL on the disk image meets several requirements.

**Special domain controller installation process** You cannot deploy preconfigured domain controllers by using image-based installation. However, you can configure a domain controller by first deploying a member server and then automatically running a script that runs Dcpromo.exe, the Active Directory Installation Wizard.

**Limited configuration of some security settings** You cannot use image-based installation to deploy computers that contain any files that are encrypted using Encrypting File System (EFS). In addition, you cannot use image-based installation to deploy systems that have already been configured with NTFS security settings, such as file and folder permissions, unless the disk-imaging program supports the NTFS file system. You can use a script to configure these settings after the image-based installation is complete.

## Terms and Definitions

The following key terms are associated with image-based installation and Sysprep.

**Mini-Setup** A wizard that is a subset of Windows Setup. Mini-Setup provides prompts for user-specific information, configures operating system settings, and detects new hardware. You can automate Mini-Setup by using Sysprep.inf.

**Factory mode** A network-enabled state that allows you to perform installation and configuration tasks before you prepare the computer for final delivery to an end user. To use Factory mode, you must make sure Factory.exe is in the same folder as Sysprep.exe and Setupcl.exe. To put a computer into Factory mode, use the **-factory** parameter when you run Sysprep.

**Sysprep.inf** An answer file that you can use to automate Mini-Setup, configure system settings, and perform installation tasks. For example, you can configure Sysprep.inf to automatically set display options, join the computer to a domain, or set telephony options. You can also configure Sysprep.inf to run scripts, programs, or commands after Mini-Setup runs. The Sysprep.inf file must exist on the hard disk of the destination computer (in the *systemdrive*\Sysprep folder).

**Winbom.ini** An answer file that you can use to automate tasks when a computer is started in Factory mode. The Winbom.ini file can exist in one of several locations, including: the hard disk of the destination computer, a removable disk, or a CD.

**Cmdlines.txt** A configurable text file that is used to customize an image-based installation. Cmdlines.txt contains a list of commands that run synchronously after Mini-Setup runs, but before a computer restarts. Cmdlines.txt must exist in the *systemdrive*\Sysprep\SOEM\$ folder on the destination computer's hard disk, and the path to Cmdlines.txt must be specified by the InstallFilePath parameter, which is in the [Unattended] section of Sysprep.inf.

**GuiRunOnce** A section in Sysprep.inf that is used to customize an image-based installation. The [GuiRunOnce] section contains a list of commands that run synchronously after a destination computer is started for the first time and a user logs on.

## New in Sysprep

Sysprep has several new features that are useful for image-based installations in corporate environments. Table 3.1 summarizes the new features.

**Table 3.1 New Sysprep Features**

Feature	Description
Cancel restart support	A Sysprep parameter that prevents a computer from restarting after you run Sysprep. This parameter is mainly used for testing, especially to check if the registry was modified correctly after you perform installation tasks.
Countdown timer setting for product activation	A Sysprep parameter that prevents a reset of the countdown timer for product activation. By default, the countdown timer for product activation is reset when you run Sysprep. This parameter is useful if you activate a computer before you deliver it to an end user. This setting is not relevant if you have a volume license.
Mass storage support	A Sysprep parameter (-bmsd) and an answer file entry (BuildMassStorageSection) that instructs Sysprep to build a list of drivers for mass storage controllers. This prevents you from having to enter device driver information manually in the Sysprep answer file, if an image supports more than one type of mass storage controller.
Device driver cleanup support	A Sysprep parameter that clears unused mass storage drivers added by the [SysprepMassStorage] section of Sysprep.inf, and removes phantom devices created by Plug and Play.

(continued)

**Table 3.1 New Sysprep Features (continued)**

Feature	Description
Audit support	A Sysprep parameter that lets you verify software and hardware installation without generating new SIDs or processing any items in the Factory mode answer file (Winbom.ini). You can only use audit support with the new Factory mode feature.
Factory mode	A Sysprep parameter that restarts a computer in a network-enabled state without running Mini-Setup. Factory mode is useful for updating drivers, running Plug and Play enumeration, installing applications, testing, configuring the computer with customer data, or making other configuration changes before you deliver a computer to an end user. The Factory mode answer file, Winbom.ini, allows you to automate many installation tasks.
Forced shutdown support	A Sysprep parameter that forces a computer to shut down after you run Sysprep. This parameter is useful if a computer has an Advanced Configuration and Power Interface (ACPI) BIOS and it does not shut down properly when you run Sysprep.
Reseal support	A Sysprep parameter that clears the Event Viewer logs and prepares the computer for delivery to the customer. Typically, you use the <code>-reseal</code> parameter after you perform installation and auditing tasks in Factory mode.

In addition, the Sysprep answer file (Sysprep.inf) has several changes that affect the way you perform an image-based installation. For more information about the changes in Sysprep.inf, see the *Microsoft Windows Corporate Deployment Tools User's Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.

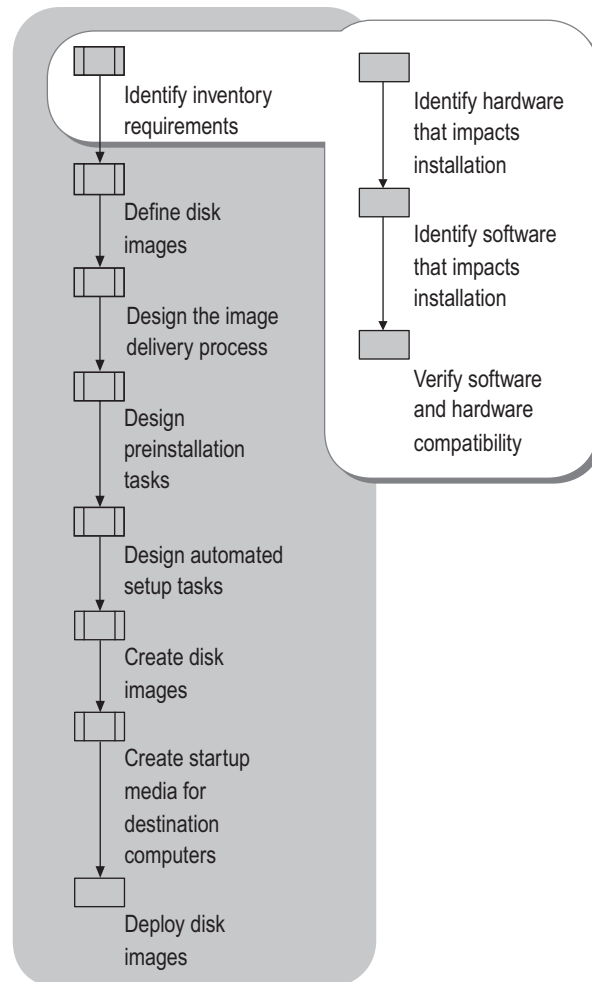
## Identifying Inventory Requirements for Image-based Installations

Before you can plan and design a deployment that uses image-based installation, you need to update your hardware and software inventories to identify hardware and software that can affect the way you perform an image-based installation and verify that all hardware and software is compatible with the new operating system. If you do not take this hardware and software into account while you are planning and designing an image-based installation, the installation might fail.

The hardware and software described in this section must be listed in your hardware and software inventories. If you do not already have hardware and software inventories, you must create them before you can plan and design your image-based installation. For more information about creating a hardware or software inventory, see “Planning for Deployment” in *Planning, Testing, and Piloting Deployment Projects* of this kit.

Figure 3.2 shows the process that you must follow to ensure that your hardware and software inventories are up-to-date and contain the information you need to design an image-based installation.

**Figure 3.2 Identifying Inventory Requirements**



## Identifying Hardware That Impacts Image-based Installations

Most Plug and Play peripheral devices, such as sound cards, network adapters, modems, and video cards, do not impact image-based installations. You do not need to inventory these types of devices because they are automatically detected, installed, and configured after you copy a disk image onto a destination computer. You do, however, need to identify several other types of peripheral devices and hardware components, including the following:

- HALs
- Mass storage controllers
- Minimum available hard disk space
- Portable computer devices
- Vendor-specific devices
- Legacy devices

### HALs

Identify how many HALs your organization uses. You can use image-based installation only if any of the following are true:

- The HAL on the master computer is identical to the HAL on the destination computer.
- The master computer has a uniprocessor or multiprocessor Advanced Programmable Interrupt Controller (APIC) HAL, and the destination computer has a uniprocessor or multiprocessor APIC HAL.
- The master computer has a uniprocessor or multiprocessor Advanced Configuration and Power Interface (ACPI) APIC HAL, and the destination computer has a uniprocessor or multiprocessor ACPI APIC HAL.

Table 3.2 lists the types of HALs that Windows XP Professional and Windows Server 2003 support.

**Table 3.2 HALs Compatible with Windows Server 2003 and Windows XP Professional**

This HAL	Can Be Used on These Computers
Non-ACPI Programmable Interrupt Controller (PIC) HAL (Hal.dll)	<ul style="list-style-type: none"> <li>Non-ACPI PIC computers</li> <li>Non-ACPI APIC uniprocessor and multiprocessor computers</li> <li>ACPI PIC computers</li> <li>ACPI APIC uniprocessor and multiprocessor computers</li> </ul>
Non-ACPI APIC uniprocessor HAL (Halapic.dll)	<ul style="list-style-type: none"> <li>Non-ACPI APIC uniprocessor computers</li> <li>ACPI APIC uniprocessor computers</li> </ul>
Non-ACPI APIC multiprocessor HAL (Halmps.dll)	<ul style="list-style-type: none"> <li>Non-ACPI APIC multiprocessor computers</li> <li>Non-ACPI APIC uniprocessor computers</li> </ul>
ACPI PIC HAL (Halacpi.dll)	<ul style="list-style-type: none"> <li>ACPI PIC computers</li> <li>ACPI APIC uniprocessor and multiprocessor computers</li> </ul>
ACPI APIC uniprocessor HAL (Halaacpi.dll)	<ul style="list-style-type: none"> <li>ACPI APIC uniprocessor computers</li> </ul>
ACPI APIC multiprocessor HAL (Halmacpi.dll)	<ul style="list-style-type: none"> <li>ACPI multiprocessor computers</li> <li>ACPI uniprocessor computers</li> </ul>

The type of HAL that is installed on a computer is often dependent on the BIOS. Before you determine the type of HAL a computer needs, make sure that the BIOS is current. For example, a computer might have ACPI-compatible peripherals, but if the BIOS is old and is not ACPI-compatible, the computer could still have a non-ACPI HAL because Setup installs the HAL based on the capabilities of the BIOS. For more information about ACPI-compatible HALs, see article Q216573, “How Windows Determines ACPI Compatibility,” in the Microsoft Knowledge Base. For more information about determining the type of HAL that is installed on a computer, see article Q298898, “How to Determine the Hardware Abstraction Layer (HAL) That Is Used in Windows XP,” in the Microsoft Knowledge Base. To find these articles, see the Microsoft Knowledge Base link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.



► **To determine the type of HAL that is installed on a computer**

1. In Windows Explorer, open the *Systemroot\System32* folder.
2. Right-click **Hal.dll**, and then click **Properties** on the shortcut menu.
3. On the **Version** tab, in the **Item name** list, click **Original file name**.
4. Use the file name of the HAL and Table 3.2 to determine the type of HAL that is installed on the computer.

You cannot use the command prompt or the Microsoft® MS-DOS® operating system to determine the type of HAL that is installed on a computer.

For more information about HAL compatibility and image-based installations, see “Reducing the Number of Master Images for Computers with Multiprocessors” in the *Microsoft Windows Corporate Deployment Tools User’s Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.

**Mass storage controllers**

You might need to identify certain types of mass storage controllers that are used in your organization. In the past, you had to create a separate disk image for each mass storage controller. This is no longer true with Windows XP Professional and Windows Server 2003; however, if you have a type of mass storage controller that is not listed in any of the device information (.inf) files that ship with Windows Server 2003 or Windows XP Professional — Machine.inf, Scsi.inf, Pnp SCSI.inf, or Mshdc.inf — you need to use the following information when you design automated setup tasks for the Mini-Setup stage of an image-based installation:

- The hard disk controller’s description, as specified in its .inf file (for example, Intel 82371AB/EB PCI Bus Master IDE Controller).
- The hard disk controller’s Plug and Play ID, as specified in its .inf file (for example, PCI\VEN\_8086&DEV\_7111).
- The file name of the hard disk controller’s .inf file.
- Driver file names for the hard disk controller. This includes the following files: *Driver.sys*, *Driver.inf*, *Driver.dll*, *Driver.cat*, and *Txtsetup.oem*, where *Driver* is the name of the device driver. Some drivers, such as small computer system interface (SCSI) miniport drivers, might not have a .dll file.
- The name of the tag file (also known as a disk tag), whose presence on a floppy disk or CD tells the driver installation program that the floppy disk or CD containing the device drivers is inserted into the floppy disk drive or CD-ROM drive. The name of the tag file is specified in the hard disk controller’s *Txtsetup.oem* file.

For a worksheet to help you record information about your mass storage controllers, see “Mass Storage Controller Worksheet” (ACISYS\_2.doc) on the *Microsoft® Windows® Server 2003 Deployment Kit* companion CD (or see “Mass Storage Controller Worksheet” on the Web at <http://www.microsoft.com/reskit>). For more information about mass storage controller compatibility and image-based installations, see “Reducing the Number of Master Images for Computers with Different Mass Storage Controllers” in the *Microsoft Windows Corporate Deployment Tools User’s Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.

### **Minimum available hard disk space**

Identify the smallest hard disk, or the smallest partition, that you plan to distribute each disk image to. This is important from a design standpoint because your disk image must be smaller than the minimum space that is available on a destination computer. By making your disk image smaller than the smallest disk or smallest partition in your organization, you make the image more versatile.

Although most disk-imaging programs can extend or shrink a partition to fit the size of the disk image, using a disk-imaging program to do so is not recommended if the disks are formatted with NTFS. Instead of having a third-party disk-imaging program extend a partition, you can have Windows extend it. This will ensure that NTFS is not compromised. For more information about extending the size of a partition, see “Automating Tasks Before Mini-Setup” later in this chapter.

### **Portable computer devices**

Identify any special devices that are installed on portable computers. Some devices are compatible only with portable computers and cannot be installed on desktop computers. For example, if you create a disk image of a portable computer that has an inboard (built-in) pointing device, such as a trackpad, and you distribute the image to a desktop computer, the desktop computer might not have any support for the mouse or keyboard during the Mini-Setup phase of an image-based installation. To prevent this behavior, create a separate disk image for portable computers.

The primary portable devices that you need to identify are:

- DVD, CD-RW, and CD-ROM drives that require vendor-specific or third-party drivers and codecs.
- Human input devices, such as trackpads and track sticks, that require vendor-specific or third-party drivers.
- Inboard or motherboard-resident devices — such as display adapters, network adapters, modems, infrared ports, and sound cards — that require vendor-specific or third-party drivers.

**Vendor-specific devices**

Identify special devices that require vendor-specific device drivers or third-party device drivers that are not available with Windows XP Professional or Windows Server 2003. Examples of these devices include smart card readers, redundant array of independent disks (RAID) controllers, flash disk devices, and IEEE 1394 bus host controllers. You might need to create a separate disk image that contains these device drivers, or you might need to install these devices after you copy a disk image onto a destination computer.

**Legacy devices**

Identify all legacy devices that are installed and used in your organization. Legacy devices are devices that do not support Plug and Play and might require manual installation and configuration after a disk image is copied onto a computer. Legacy devices do not necessarily require you to create separate disk images, but they can force you to alter the way you perform an image-based installation. For example, you can create a disk image for computers that have only Plug and Play devices, but still use that disk image on computers that have non-Plug and Play devices. For those computers that have non-Plug and Play devices, you might have to run a script after Mini-Setup to configure the non-Plug and Play device settings. For more information, see “Automating Tasks After Mini-Setup” later in this chapter.

---

## Identifying Software That Impacts Image-based Installations

Several types of software can affect the way you perform an image-based installation. Some applications cannot be installed and configured on a disk image; they must be installed after the disk image is copied onto a destination computer. Some applications can only be installed on portable computers and cannot be installed on desktop computers, which can force you to create separate disk images for portable and desktop computers. To determine whether your software impacts your image-based installation, identify which of the following types of software you need to install.

**Core applications**

Identify the core applications that you want installed on every client and server computer. For client computers, this typically includes an office productivity suite, which includes such applications as an e-mail client, a spreadsheet, and a word processor. For server computers, this typically includes tools for maintenance and operations, such as performance-monitoring applications, remote management programs, and backup programs. Virus-detection programs are also core applications because they are usually installed on all computers.

Core applications are typically installed and configured on the disk image. If there are any computers that you do not want to install core applications onto, or any computers require different configuration settings for the core applications, note this in your software inventory.

**Line-of-business applications**

Identify all of the line-of-business applications that are used in your organization, and identify which groups use them. Accounting programs, specialized database programs, and investment modeling programs are examples of line-of-business applications. You might want to create a separate disk image for certain groups if they use line-of-business applications that require substantial configuration or take a long time to install.

**Applications that depend on Active Directory**

Identify all applications that are dependent on Active Directory. These applications cannot be installed and configured on a disk image: you must install and configure these applications after the disk image is copied onto a destination computer. An application is dependent on Active Directory if it uses any data from Active Directory or writes any data to Active Directory when the application is installed or when the application is run. You do not need to identify applications that are built into the operating system, such as snap-ins, optional components, or system tools.

**Third-party tools**

Identify all third-party tools that are specific to a certain computer or hardware configuration. For example, many computer manufacturers have a suite of diagnostic tools that are designed for their specific computers. Likewise, portable computers commonly have a suite of hardware-specific tools that let you configure power options and other features. You might need to install these tools after the disk image is copied onto destination computers, or you might want to create a separate disk image for the computers that require these tools.

**Service packs, hotfixes, and patches**

Identify all service packs, hotfixes, and patches that are installed in your organization. Be sure you record the revision number and the revision date of the service pack, hotfix, or patch.

Having this information in your software inventory makes subsequent design steps easier for you to perform. If you do not have a software inventory, or you need to update your software inventory, keep these tips in mind:

- Be sure to allow plenty of time for preparing your software inventory. Customer data shows that you and your administrative staff might spend considerably more time identifying the software that is used in your organization than you estimate.
- Do not rely on end-user feedback to create a software inventory. End users often do not know what programs they use, because some programs do not have a user interface and some programs start without end-user interaction.
- Create a database for your software inventory and keep the database updated. You can use the database to plan, design, and track rollouts of service packs, hotfixes, and patches.

## Verifying Software and Hardware Compatibility

As with any operating system installation, you need to make sure that your software and hardware are compatible with the new version of the operating system. You can use any of the following tools to check hardware and software compatibility.

### Windows Catalog

Windows Catalog contains a list of software and hardware products that are designed for, or are compatible with, Windows XP Professional. You can search the catalog by manufacturer, product type, product name, or model. If you do not see a product in the Windows Catalog, it does not mean the product will not work with the Microsoft® Windows® XP family of operating systems — check with the product's manufacturer to determine whether the product works with Windows XP. To use the Windows Catalog, see the Windows Catalog link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

### Upgrade Advisor

Windows XP Upgrade Advisor and Windows Upgrade Advisor are tools that check your system hardware and software to see whether they are ready to be upgraded to Windows XP Professional or Windows Server 2003. Although these tools are designed for use in upgrading to Windows XP Professional or Windows Server 2003, you can use them to identify software and hardware that is not compatible with a clean installation of Windows XP Professional or Windows Server 2003. To download the Upgrade Advisor tools, see the Windows Upgrade Advisor link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>. You can also run the Upgrade Advisor tools by using the **/checkupgradeonly** parameter with the Winnt32.exe tool. The Winnt32.exe tool is included in the I386 folder on the Windows XP Professional and Windows Server 2003 operating system CD.

### Application Compatibility Toolkit

The Application Compatibility Toolkit contains documents and tools to help you diagnose and resolve application compatibility issues. For more information about the Application Compatibility Toolkit, see article Q294895, "Description of the Application Compatibility Toolkit 2.0 for Windows XP," 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>.

## Defining Disk Images

A disk image contains the operating system, software applications, and configuration settings that you want to copy onto a group of computers. Most corporate rollouts, regardless of size, require more than one disk image. However, it is a good idea to minimize the number of disk images your organization uses. Creating and maintaining a disk image is time-consuming and requires ongoing maintenance as your organization's hardware and software needs change. Having fewer disk images reduces the total cost of ownership and simplifies the deployment process.

Several factors influence how many disk images you need.

**Operating system versions** You need to create a separate disk image for each version of the operating system you are deploying. For example, if you are deploying Windows XP Professional, Windows Server 2003, Standard Edition, and Windows Server 2003, Web Edition, you will need at least three disk images.

**Hardware** You might have to create additional disk images if the destination computers have different peripheral devices or hardware configurations. For example, you cannot copy a disk image that contains an ACPI HAL onto a computer that requires a non-ACPI HAL. In this case, you have to create separate images for an ACPI HAL and a non-ACPI HAL. Portable computers are another example of hardware that commonly requires a separate disk image.

**Software** You might have to create additional disk images if you are deploying different software configurations and you do not want to install and configure software after the image-based installation is complete. You might also have to create additional disk images if you need to install proprietary line-of-business applications or special tools onto a specific group of computers (for example, portable computers).

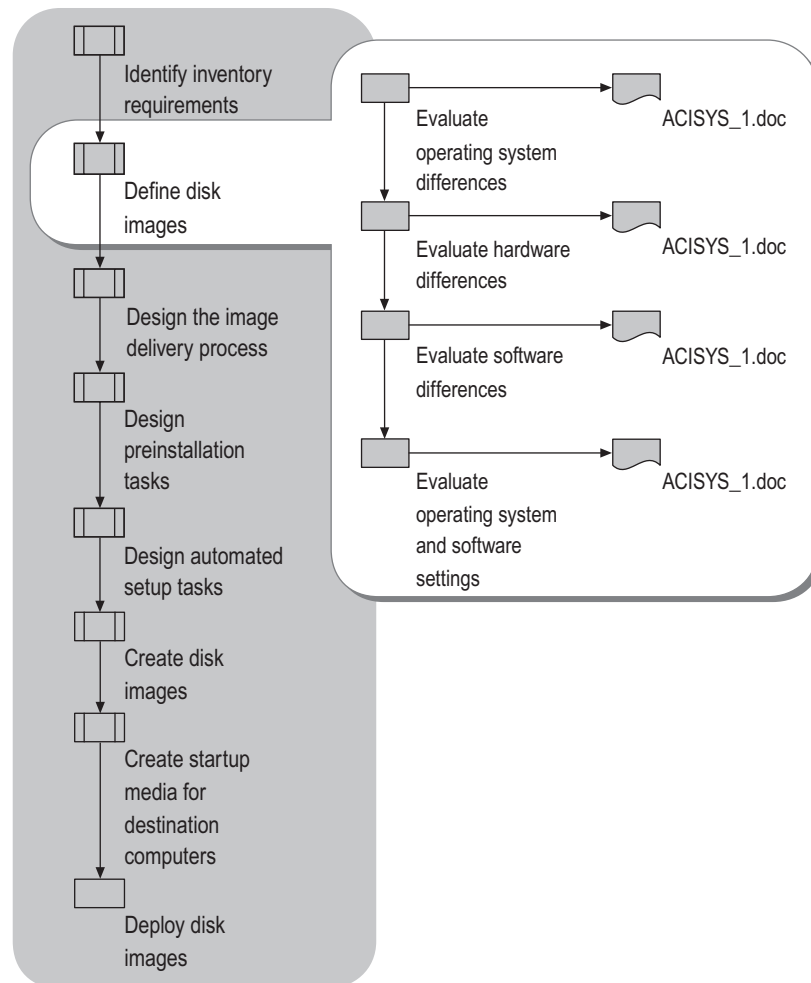
**Operating system and software settings** You might want to create additional disk images for computers that require special operating system or software settings. For example, if you want to configure special local policy settings for a group of computers, and you do not want to do this by using a script after the image-based installation is complete, you can create a separate disk image that includes the special policy settings for that group of computers.

In addition to reducing the number of disk images you need to maintain, try to reduce the size of your disk images. This reduces the time it takes to transfer disk images across a network, and it reduces the time it takes to create disk images of your master computers. For more information about reducing the size of your disk images, see "Optimizing Your Images" in the *Microsoft Windows Corporate Deployment Tools User's Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.

For a worksheet to help you in defining your disk images, see “Disk Image Worksheet” (ACISYS\_1.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Disk Image Worksheet” on the Web at <http://www.microsoft.com/reskit>). You will need a separate copy of the worksheet for each disk image. You will also need the information from your software and hardware inventories to define your disk images.

Figure 3.3 shows the design steps you need to follow to define your disk images.

**Figure 3.3 Defining Disk Images**



## Evaluating Operating System Differences

To start defining your images, create a copy of the job aid “Disk Image Worksheet” (ACISYS\_1.doc) for each operating system you are deploying. Under “Operating System Installed on This Image,” enter the product name, the full version number of the operating system, and any service packs, security updates, or fixes that you want to include in each disk image. If you are testing preliminary installations of the operating systems you plan to deploy — and you have installed all of the service packs, security updates, and fixes on your test computers — you can get a comprehensive listing of this information by running the **systeminfo** command at the command prompt. If you do not know which service packs, security updates, or fixes are available for the operating systems you plan to deploy, you can use Windows Update to determine this information. For more information about Windows Update, see the Windows Update link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

---

## Evaluating Hardware Differences

You might need to create separate disk images if your computers have different hardware configurations. To determine whether you need additional disk images based on your hardware configurations, you need to evaluate the following categories of hardware.

### HALs

You can only copy a disk image onto a destination computer if the HAL on the disk image is compatible with the HAL on the destination computer. Compatible HALs are those that are identical or those that can be updated during an image-based installation. If the HAL on your disk image is not compatible with the HAL that is required on a destination computer, you need to create a separate disk image for the HAL that is required on the destination computer. Table 3.2 can help you determine which HALs are compatible.



### Caution

Copying a disk image to a destination computer that has an incompatible HAL can cause the destination computer to restart continuously, become unresponsive, or generate Stop errors.

Using the information in your hardware inventory, you can determine whether you need more than one disk image for each operating system based on your HAL requirements. For example, if you are installing Windows Server 2003, Standard Edition on 50 computers, 10 of which require a non-ACPI HAL and 40 of which require an ACPI HAL, you need to create two disk images of Windows Server 2003, Standard Edition: one image for the ACPI HAL and one image for the non-ACPI HAL.



Use the following guidelines to determine how many disk images you need based on the HALs used in your organization:

- PIC and APIC HALs are not compatible: You need one disk image for computers that require PIC HALs and one disk image for computers that require APIC HALs.
- ACPI and non-ACPI HALs are not compatible: You need one disk image for computers that require ACPI HALs and one disk image for computers that require non-ACPI HALs.
- Non-ACPI APIC uniprocessor HALs and non-ACPI APIC multiprocessor HALs are compatible: You can use a single disk image for all computers that require these HALs.
- ACPI APIC uniprocessor HALs and ACPI APIC multiprocessor HALs are compatible: You can use a single disk image for all computers that require these HALs.
- ACPI PIC HALs are not compatible with any other HAL: You need a separate disk image for computers that require ACPI PIC HALs.

In addition, you might need to have a separate disk image if any of your computers support hyper-threading. Hyper-threading enables multithreaded software applications to execute threads in parallel within each processor. On a hyper-threading enabled system, Windows XP and the Windows Server 2003 family function as they would on a multi-processor system, even when only a single physical processor is installed.

Windows automatically uses the hyper-threading capabilities of the processor if the following conditions are met:

- The computer hardware supports hyper-threading, and this functionality is enabled in the computer's BIOS.
- Hyper-threading functionality is installed in the computer processor.
- The computer is using an ACPI Uniprocessor HAL.
- Windows detects one or more processors or enabled threads.

When the listed conditions are met, Windows automatically updates the HAL to the ACPI Multiprocessor HAL and installs an additional processor.

When a disk image is copied to a hyper-threading-enabled system, and the HAL is incompatible, the computer might not boot correctly. If the computer does boot correctly, it might not be able to take advantage of hyper-threading technology.

To ensure that the HALs on your disk images are compatible with hyper-threading enabled systems, you must create the master installation on a computer that has one of the following:

- An ACPI hyper-threading enabled HAL.
- An ACPI APIC uniprocessor HAL.
- An ACPI multiprocessor HAL.

If you do not create the master installation on one of these types of computers, Windows is not able to update the system to use multiple processors. A Sysprep image made on an ACPI-compliant multiprocessor computer will run in a multiprocessor configuration even if support for hyper-threading is turned off in the BIOS.

In each copy of the job aid “Disk Image Worksheet ” (ACISYS\_1.doc), under “Hardware Installed on this Image,” enter the type of HAL that will be included on the disk image. You might have to create more copies of the worksheet if you are deploying several different types of HALs with the same operating system and the HALs are incompatible. Be sure to include the file name of the HAL in the worksheet. HAL file names and descriptions are listed in Table 3.2.

### **Portable computer devices**

You might also need to create a separate disk image for portable computers. Portable computers often require vendor-specific or hardware-specific device drivers. Frequently, these specialized device drivers are not compatible with desktop computers. For example, if you configure a disk image of a portable computer that has an inboard pointing device, and then copy the disk image onto a desktop computer, the desktop computer might not have mouse or keyboard support.

If the portable computers in your organization require special device drivers, consider creating separate disk images for your portable computers. Having separate disk images for your portable computers prevents device conflicts and ensures that the appropriate device drivers are installed on both your portable and desktop computers.

In each copy of the worksheet under “Hardware Installed on this Image,” record the names of the portable devices the disk image supports and the names of the device driver files that are associated with the devices. You might have to create more copies of the worksheet if you decide to create separate disk images for your portable computers.

### **Other devices**

You do not need to create separate disk images for legacy (non-Plug and Play) hardware or hardware that requires vendor-specific device drivers; however, you might want to do this if you have a large number of computers that require the same special device drivers and have the same hardware configuration. For example, you might want to create a separate disk image for file servers that have RAID storage devices. Frequently, you have to install vendor-specific drivers for RAID devices, and you have to use a vendor-specific utility to configure them. Having a separate disk image lets you copy a fully configured and optimized system without having to perform any configuration tasks after deployment.

You can use your hardware inventory to identify legacy devices or other devices that require vendor-specific device drivers. In each copy of the worksheet under “Hardware Installed on this Image,” record the names of any legacy devices and vendor-specific devices a disk image supports. Also include the names of all files that are associated with the device drivers.

**Mass storage controllers**

You do not need a separate disk image for each mass storage controller. However, you need to make sure that the appropriate device drivers for a mass storage controller are available on a disk image or on a floppy disk. If a mass storage controller is listed in the device information files that ship with Windows Server 2003 and Windows XP Professional — Machine.inf, Scsi.inf, Pnp SCSI.inf, or Mshdc.inf — then the device drivers for it will be available on the disk image. If the mass storage controller is not listed in one of these .inf files, you need to record the name of the mass storage controller under “Hardware Installed on this Image.” If the mass storage controller is not listed in the “Mass Storage Controller Worksheet” (ACISYS\_2.doc), you also need to record the following information for the mass storage controller under “Hardware Installed on this Image”: the Plug and Play device ID, the names of the device driver files, the tag file or disk tag, and the name of the .inf file.

---

## Evaluating Software Differences

You do not need to create a separate disk image for every computer that has a different software configuration. You can automatically install and configure most software applications after you copy a disk image onto a destination computer (for more information about automatically installing applications at the end of an image-based installation, see “Automating Tasks After Mini-Setup” later in this chapter). This reduces the number of disk images you have to manage, and it makes it easier for you to modify a software configuration as the needs of a group change.

Still, you might want to create a separate disk image based on a specific software configuration when the following conditions exist:

- A group of computers requires software applications or tools that conflict with other software programs. For example, you might want to create a separate disk image for portable computers that require the same vendor-specific programs, such as power-management utilities, DVD codecs, or diagnostic tools.
- A group of computers requires software applications that cannot be automatically installed and configured after the disk image is copied onto a destination computer. For example, you might want to create a separate disk image for Web servers that all run the same suite of third-party data analysis and monitoring applications. This ensures that all of your Web servers have a consistent configuration, and it eliminates the need to manually install and configure third-party applications after you copy a disk image onto a Web server.
- A group of computers requires that the same unique software configuration be installed frequently. For example, you might want to create separate disk images for trade-show kiosks or computers that are used for training purposes, because these computers require frequent reinstallation.

Regardless of whether or not you create separate disk images for specific software configurations, you need to determine which software applications you want to include on a disk image and which software applications you want to install after the disk image is copied onto a destination computer. You can use your software inventory in conjunction with the following design guidelines to define a software configuration for each disk image.

**Identify core applications** Identify the applications that you want installed on every computer, then install and configure these applications on the disk image. Record the names of the programs in each worksheet under “Software Installed on This Image.”

**Identify service packs, hotfixes, and patches** It is a good idea to install and configure service packs, hotfixes, and patches on the disk image. Service packs often take a long time to install; it is more efficient to install them on the disk image. Record the names and versions of service packs, hotfixes, and patches in each worksheet under “Operating System Installed on This Image.” Keep in mind that if you install any applications after the disk image is copied onto a destination computer, you might have to install service packs, hotfixes, and patches after the disk image is copied onto a destination computer. Record this information in each worksheet under “Software Installed After Disk Copy.”

**Identify applications that cannot be installed on a disk image** You must install and configure some applications after you copy a disk image to a destination computer and Mini-Setup has finished running. This includes: programs that depend on Active Directory, such as Message Queuing (also known as MSMQ); special server applications, such as Certificate Services and Cluster service; and special applications that you want installed only on certain computers or certain groups of computers. Record the names of these programs in each copy of the worksheet under “Software Installed After Disk Copy.”

Do not include information about configuration settings in the worksheet at this point. You will evaluate and record configuration settings later in this chapter.



#### Note

The Sysdiff.exe tool is not available for Windows XP Professional or Windows Server 2003. If you used Sysdiff.exe to deploy Microsoft® Windows® 2000 or Windows NT® version 4.0 operating systems, and you need a tool with similar functionality, you need to find another tool. For more information about other resources that are similar to Sysdiff.exe, see article Q298389, “Sysdiff.exe Deployment Tool Is Not Included in Windows XP,” 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>.

## Evaluating Operating System and Software Settings

You do not usually need to create a separate disk image for each computer or group of computers that has different operating system settings or different software settings. You can configure most operating system and software settings on the master computer before you create the disk image. However, if you need to configure settings that are unique, you can automatically configure the settings during Mini-Setup while the destination computer is being set up, or after Mini-Setup is complete and the destination computer has been restarted.

Examples of operating system and software settings include:

- Local policy settings, such as Group Policy Administrative Template settings.
- Control Panel settings, such as power options, sound scheme settings, system startup and recovery options, system performance settings, and accessibility options.
- Internet Explorer settings, such as the default home page, security and privacy settings, and connection settings.
- Optional Windows components settings, such as network monitoring tools, Remote Storage, and Services for Macintosh.
- Services settings, such as startup type, logon accounts, and recovery actions.
- Desktop settings, such as desktop shortcuts and folder options.
- Microsoft® Word or Microsoft® Excel settings, such as view, edit, save, and spelling options.

You can record operating system settings in each copy of the worksheet under “Operating System Installed on This Image” and under “Operating System Settings Configured After Disk Copy.” Likewise, you can record software configuration settings in each worksheet under “Software Installed on This Image” and under “Software Installed After Disk Copy.”

Most operating system settings and software settings can be configured on the master computer before you create the disk image. However, you must configure the following settings after the disk image is copied onto a destination computer.

**Domain controller settings** You cannot configure a master computer as a domain controller. You first configure a master computer as a member server, and then configure it as a domain controller after the disk image is copied onto a destination computer. You use Dcpromo.exe (also known as the Install Active Directory Wizard) to configure a server as a domain controller.

**Plug and Play hardware settings** You must configure settings for Plug and Play hardware after a disk image is copied onto a destination computer. For example, you cannot configure power management settings for a specific device, such as enabling wake-on-LAN settings for a network adapter, or configuring link speed or duplex settings for a network adapter. Sysprep configures the master computer so that Plug and Play devices are detected, installed, and reconfigured with default settings the first time you start a computer after a disk image is copied onto it.

**Static IP address settings** You must configure static IP address settings after a disk image is copied onto a destination computer (by using Sysprep.inf). When a disk image is copied onto a destination computer, all of the network adapters on a destination computer are initialized to the default settings, which include dynamic allocation of IP addresses. For more information about how Sysprep affects network settings, see article Q271369, “Statically-Entered TCP/IP Settings Are Not Present After Sysprep,” 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>.

**Encrypting File System settings** You must configure EFS settings on files and folders after a disk image is copied onto a destination computer. If you run Sysprep on a hard disk that contains encrypted files or folders, the data in those files and folders will become completely unreadable and unrecoverable.

**Policy settings** You can configure local Group Policy Administrative Template settings on a master computer. This is because Administrative Template settings are stored in the registry, and Sysprep does not change this part of the registry. Any changes you make to Administrative Template settings will appear on the disk image. You can also configure other local Group Policy settings if the local Group Policy object is not linked to a site, domain, or organizational unit Group Policy object. This is because Sysprep does not change the local Group Policy object as long as local Group Policy settings are not overridden by site, domain, or organization unit Group Policy settings. If Group Policy settings are not overridden by site, domain, or organizational unit Group Policy settings, any changes you make to local Group Policy settings will appear on the disk image. If the local Group Policy settings are overridden by site, domain, or organizational unit Group Policy settings, and you configure these settings on a master computer, the settings will be overridden on each destination computer.

**Mini-Setup settings** Several types of operating system settings are configured during Mini-Setup. Examples of these settings include: telephony settings, licensing information, computer name, administrative password, and domain membership settings. You cannot configure Mini-Setup settings on the master computer before you create the disk image. For more information about Mini-Setup settings, see “Designing Automated Setup Tasks” later in this chapter.

---

## Designing the Image Delivery Process

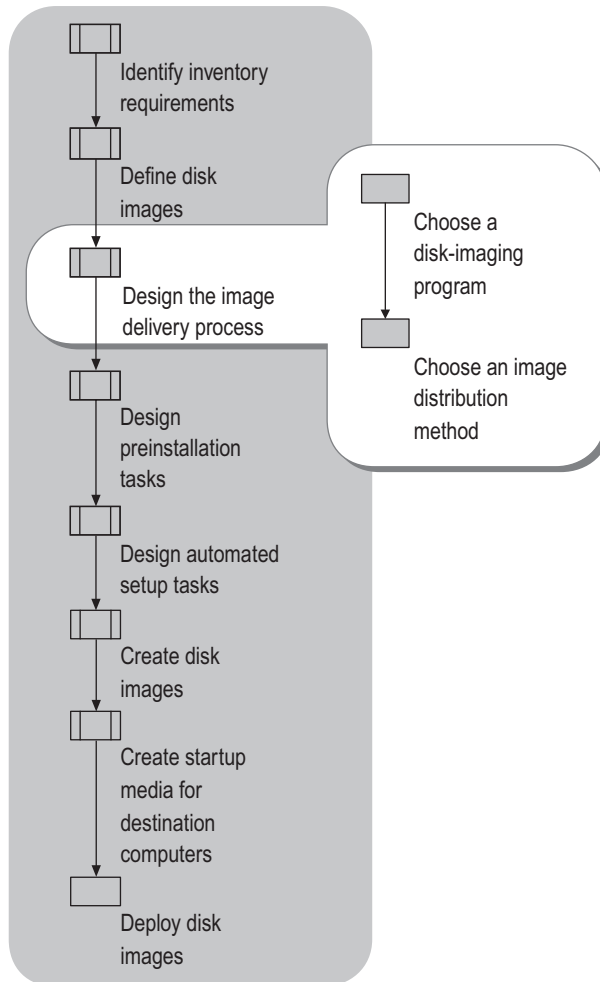
*Image delivery* is the process of creating, managing, and distributing disk images. The image delivery process begins after you configure your master computer, and it ends after you copy a disk image onto a destination computer. To design an effective image delivery process, perform the following tasks:

- Choose a disk-imaging program, which you will use to create and manage disk images.
- Choose an image-distribution method, which you will use to store and transfer disk images to destination computers.

Your disk-imaging program must be compatible with the operating system and file system you are deploying, and your distribution method must be compatible with your organization's networking and hardware capabilities.

Figure 3.4 shows the steps to follow in designing your image delivery process.

**Figure 3.4 Designing the Image Delivery Process**



## Choosing a Disk-Imaging Program

Microsoft does not provide disk-imaging software. You must purchase a third-party disk-imaging program to create a disk image of a master computer's hard disk.

Not all disk-imaging programs are compatible with Windows Server 2003 and Windows XP Professional. When you evaluate disk-imaging programs, make sure you choose a program that supports the following Windows Server 2003 and Windows XP Professional features:

- **Long file names.** Be sure your disk-imaging program supports long file names. (Long file names can be up to 255 characters and can contain spaces, multiple periods, and special characters that are not allowed in MS-DOS file names.) Most commercial third-party disk-imaging programs can handle long file names, but some shareware and freeware disk-imaging programs cannot.
- **NTFS 3.1.** Be sure that your disk-imaging program supports NTFS 3.1, which is the version of NTFS used by Windows Server 2003 and Windows XP Professional. Although many disk-imaging programs support NTFS, these programs do not necessarily support the new features in NTFS 3.1, such as the clean shutdown flag.

In addition to these required features, consider choosing a disk-imaging program that supports the following optional features:

- **Network share support.** Some disk-imaging programs can copy disk images to and from network shares. This feature is essential if you distribute disk images across a network.
- **CD-RW support.** Some disk-imaging programs can write the disk image directly to a writable CD. This feature is useful if you distribute disk images on CDs.
- **Large-file support (also known as file splitting or disk spanning).** Some disk-imaging programs can copy an image onto multiple CDs or other media. This is useful because a typical disk image of Windows Server 2003 or Windows XP Professional does not fit on one CD.
- **Stand-alone support.** Some disk-imaging programs provide a mechanism for booting a computer that is not connected to a network, and then copying an image from removable media without using a network connection. This is useful if you distribute your disk images on CD or DVD.
- **Multicast image deployment.** Some disk-imaging programs have a multicast server feature that lets you simultaneously copy a disk image onto multiple computers over a network connection. This is useful for large-scale rollouts where you want to automate and control the disk copy process.
- **Image management.** Some disk-imaging programs have image-management features that let you view, add, and remove files and folders from a disk image. This is useful for updating a disk image without having to reconfigure a master computer and create a new disk image.



Some disk-imaging programs can create, resize, or extend a partition before you copy a disk image onto a destination computer. Although these features might be useful, not all disk-imaging programs can perform these tasks: in fact, some programs might cause a STOP 0x7B error (INACCESSIBLE\_BOOT\_DEVICE). If you want to create a partition on a destination computer's hard disk before you perform an image-based installation, you need to be sure the disk-imaging program is compatible with the file systems used by Windows Server 2003 and Windows XP Professional. If you want to resize or extend a partition before you copy a disk image onto a destination computer, use the ExtendOemPartition parameter in the Sysprep.inf file.

For more information about Stop 0x7B errors, see article Q257813, "Using Sysprep May Result in 'Stop 0x7B (Inaccessible Boot Device)' on Some Computers," 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 using the ExtendOemPartition parameter, see "Automating Tasks Before Mini-Setup" later in this chapter.

**Note**

If you are deploying a 64-bit edition of Windows XP or a 64-bit version of the Windows Server 2003 family, you must use a 64-bit disk-imaging program.

---

## Choosing an Image Distribution Method

*Image distribution* refers to the way you store a disk image and the way you transfer a disk image to a destination computer. You can distribute disk images two ways:

- You can store images on a network share and then distribute the images across the network to destination computers. This is referred to as *network distribution*.
- You can store images on media such as a CD or a DVD, and then distribute the images from the media to destination computers. This is referred to as *media distribution*.

You need to determine which distribution method to use for each of your disk images. You will likely have to use both distribution methods for some disk images. For example, you might use network distribution to roll out Windows XP Professional in a corporate office that has a high-speed local area network (LAN), but you might also use media distribution to roll out the same image in a branch office that has a slow and unreliable network connection.

## Distributing Disk Images Across a Network

To distribute disk images across a network, you need:

- High-speed network connectivity.
- Adequate file server capacity.
- A disk-imaging program that supports network distribution.
- A network boot disk.

Network distribution might also require additional administrative overhead, such as network configuration and troubleshooting, file server configuration and management, and security configuration. For example, you might have to configure network settings or troubleshoot network issues if a destination computer cannot access the network. Likewise, you might have to add storage capacity to your file servers and address performance issues to ensure that your file servers are optimally configured for handling disk images. You might also have to configure permissions, security policies, or user rights on your file servers so that unauthorized users do not download or copy your disk images.

### High-speed network connectivity

You must have a network connection to every destination computer that you are deploying. Ethernet LANs and Token Ring LANs are well-suited for distributing disk images across a network. Wide area networks (WANs) are generally not fast enough, unless the LAN segments that make up the WAN are connected with a fast T-Carrier service (T2 or higher). Digital subscriber line (DSL), cable modem, Integrated Services Digital Network (ISDN), and dial-up modem connections are not suitable for network distribution.

Table 3.3 shows disk image transfer times based on connection type and network speed. Image transfer times are based on optimum network speeds only and are calculated for a 2.5 gigabyte (GB) disk image. File server performance is not factored into the disk image transfer times. You can use Table 3.3 as a rough guide to help you determine whether your network is a suitable for network distribution.

**Table 3.3 Disk Image Transfer Times Based on Connection Type and Network Speed**

Connection Type	Network Speed	Transfer Time (2.5 GB Disk Image)
Fast Ethernet	100 Megabits per second (Mbps)	3 minutes, 25 seconds
Fast Token Ring	16 Mbps	21 minutes, 22 seconds
Ethernet	10 Mbps	34 minutes, 9 seconds
T2	6.312 Mbps	54 minutes, 6 seconds
Token Ring	4 Mbps	1 hour, 25 minutes
T1	1.544 Mbps	3 hours, 41 minutes

**Adequate file server capacity**

You must have a file server configuration that can handle large file transfers. Several factors determine whether a file server is adequate for large file transfers. The disk type (integrated device electronics [IDE] or SCSI), disk access speed, network adapter settings, disk rotation speed, bus speed, and protocol type can all influence the performance of a file server. Many hard disk manufacturers provide applications that measure your disk performance.

**Disk-imaging program that supports network distribution**

You must have a third-party disk-imaging program that supports network deployment or transfer of disk images. Many disk-imaging programs can copy a disk image directly to a network share. Others can only copy a disk image onto a hard disk on the same computer you are imaging, which means you must manually copy the disk image to a network share. Some programs also provide network deployment features, such as a multicast feature that you can use to deploy images simultaneously to multiple destination computers, and a subnet selection feature that you can use to distribute images to selected subnets. Although these features are not required for network distribution, they can make an image-based deployment faster and easier.

**Network boot disk**

You must have a network boot disk (floppy or CD) in order to transfer disk images across the network. You use the boot disk to start the destination computer you are deploying and connect the destination computer to a network. Some third-party disk-imaging programs provide a network boot disk (floppy). You can also create one yourself. For more information about creating a network boot disk, see “Creating Startup Media” later in this chapter.

---

## **Distributing Disk Images by Using Media**

To distribute images on media, you need CD or DVD recording hardware, a disk-imaging program that supports media distribution, a file-splitting or disk-spanning program, and a boot disk with CD or DVD support.

Media distribution might also require additional administrative overhead. The most common administrative tasks associated with media distribution include: configuring and troubleshooting CD-ROM drives, maintaining and updating disk images, and managing security. For example, you might have to configure or troubleshoot CD-ROM or DVD drives if your boot disk fails to load the appropriate CD-ROM or DVD device drivers on a destination computer. Likewise, you might have to record new CDs or DVDs (and, for security purposes, destroy old CDs and DVDs) every time you make a change to your disk image. You will also spend administrative time ensuring that the CDs and DVDs are physically secure and not available to unauthorized users.

**CD or DVD recording hardware**

You must have a CD or DVD recorder to distribute images on media. You can use any type of CD or DVD recording device (for example, CD-R or CD-RW). However, you must make sure that the CD-ROM drives in your destination computers can read the media you create.

**Disk-imaging program that supports media distribution**

You must have a disk-imaging program that allows you to copy a disk image directly onto a hard disk, CD, or DVD on the same computer. Some disk-imaging programs do not support stand-alone disk image creation (for example, disk-to-disk or disk-to-CD). This feature is necessary if your master computers are not connected to a network, or you want to create distribution media immediately after you create a disk image.

**File-splitting or disk-spanning program**

Most disk images of Windows XP Professional or Windows Server 2003 will not fit on a single CD, so you will need a file-splitting or disk-spanning tool that splits a disk image into several files. Some disk-imaging programs provide this functionality, but most do not. To find vendors and shareware Web sites that offer file-splitting or disk-spanning programs, search the Web by using the keywords **file splitting** or **disk spanning**.

**Boot disk with CD or DVD support**

You must have a boot disk to start the destination computer. The boot disk can be the CD or DVD that contains the disk image, or it can be a separate floppy disk. The boot disk must also include the device drivers for the CD-ROM or DVD drive that is in the destination computer. Some third-party disk-imaging programs provide a network boot disk (floppy). You can also create one yourself. For more information about creating a network boot disk, see “Creating Startup Media” later in this chapter.

---

## Comparing Disk Image Distribution Methods

Each method of distributing disk images has advantages and disadvantages. Table 3.4 summarizes the advantages and disadvantages of each distribution method. You can use Table 3.4 to identify which distribution method is best suited for each of your disk images and your organization.

**Table 3.4 Comparison of Disk Image Distribution Methods**

Feature	Network Distribution	Media Distribution
Can be used to deploy disk images in remote offices that do not have fast network connections.	No	Yes
Can be used to deploy disk images to computers that do not have network connectivity.	No	Yes
Requires a file server with adequate capacity to store disk images.	Yes	No

(continued)

**Table 3.4 Comparison of Disk Image Distribution Methods (*continued*)**

Feature	Network Distribution	Media Distribution
Requires software-based security to prevent unauthorized access to disk images (permissions, user rights).	Yes	No
Requires physical security to prevent unauthorized access to disk images (locks on doors, locks on office desks).	No, but it is a good idea.	Yes
Accommodates disk images of any size without special file-splitting or disk-spanning software.	Yes	No
Requires CD or DVD recording hardware and media.	No	Yes

You can use the following guidelines to choose a distribution method.

Choose network distribution if all of the following statements are true:

- You are deploying computers that are connected to a fast network (> 4 Mbps).
- You have a file server with sufficient capacity to store all of your disk images.
- You have a disk-imaging program that supports network distribution of disk images.

Choose media distribution if all of the following statements are true:

- You are deploying computers that are connected to a slow network, or you are deploying computers that are not connected to a network.
- You have CD or DVD recording hardware.
- You have a disk-imaging program that supports disk-to-disk or disk-to-CD copying.

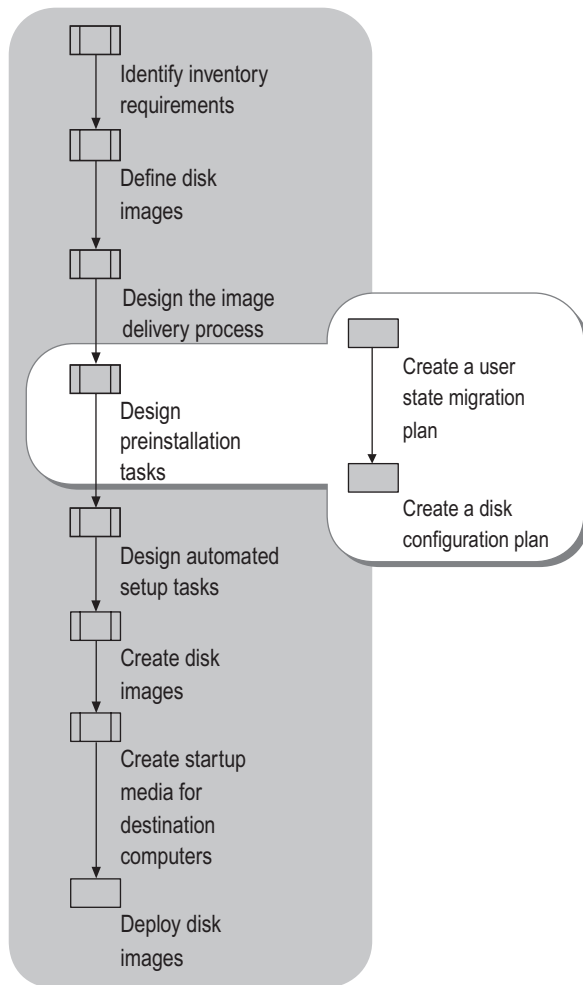
## Designing Preinstallation Tasks for Image-based Installations

After you design the image delivery process, you need to identify and plan your preinstallation tasks. Preinstallation tasks are performed before you copy a disk image onto a destination computer. You might not need to perform any preinstallation tasks; you will need to perform some preinstallation tasks if you want to:

- Migrate user state before you copy a disk image onto a destination computer. You will likely not need to do this if you use folder redirection and roaming profiles to store user data and settings on a server.
- Change the size or format of the system partition before you copy a disk image onto a destination computer. You do not need to do this if all of your hard disks are already partitioned and formatted the way you want them.

Figure 3.5 shows the steps to follow in designing your preinstallation tasks.

**Figure 3.5 Designing Preinstallation Tasks**



## Creating a User State Migration Plan for Image-based Installations

You will need to create a user state migration plan if any of your destination computers contains any of the following items that you want to restore after installation is complete:

- User data that you want to be available to the end user. User data includes such things as documents, e-mail messages, spreadsheets, and databases.
- User settings such as desktop settings, shortcuts, and Internet Explorer Favorites.
- Application settings such as application-specific keyboard shortcuts, spell-checking options, and default file locations.

At a minimum, your user state migration plan must do the following:

- Identify the data you want to migrate, including user data, user settings, and application settings.
- Determine where to store the data while you perform the image-based installation.
- Create a schedule for migrating data on each of your destination computers.
- Describe how to collect and restore the data.

Microsoft provides two tools for migrating user data and settings. Each tool is designed for different types of users and environments.

- **Files and Settings Transfer Wizard.** Designed for home users and small office users, the 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.
- **User State Migration Tool.** Designed for IT administrators who perform large deployments of Windows XP Professional in a corporate environment, the User State Migration Tool provides the same functionality as the wizard, but on a large scale targeted at migrating multiple users. The User State Migration Tool gives administrators the flexibility of a command line approach to customizing specific settings, such as registry entries. To download a free version of the tool, see the User State Migration Tool link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

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

## Creating a Disk Configuration Plan for Image-based Installations

You need to create a disk configuration plan if any of the following are true:

- You want to change the size of the system partition on your destination computers before you perform an image-based installation.
- You want to reformat the system partition on your destination computers before you perform an image-based installation.
- You want to create and format extra partitions on your destination computers before you perform an image-based installation.

You do not need to create a disk configuration plan if you configure disk settings after a disk image is copied onto a destination computer. It is relatively easy to delete, create, and format extra partitions — or extend an existing partition — and these tasks do not require substantial analysis and planning. You can automate these types of disk configuration tasks during an image-based installation by configuring parameters in `Winbom.ini` and `Sysprep.inf`.



### Note

You cannot put the system partition and boot partition on separate partitions if you use Sysprep to prepare a master computer for disk imaging: The system partition and boot partition must be on the same partition.

## Configuring Disk Settings

There are three ways to configure disk settings before you copy a disk image onto a destination computer.

**Use MS-DOS or Windows 98 disk configuration tools** You can start a destination computer by using a boot disk for MS-DOS or a boot disk for the Microsoft® Windows® 98 operating system, and then use the **fdisk** and **format** commands to partition and format the disk before you copy a disk image onto the destination computer. This method only works if you want to format your disks with the file allocation table (FAT) or FAT32 file system. If you want your hard disks formatted with NTFS, you will have to run the **convert** command by using the [GuiRunOnce] section in `Sysprep.inf` to convert the FAT or FAT32 file system to NTFS after you have copied the disk image onto the destination computer. For more information about disk partitions and file systems, see the *Server Management Guide* of the *Microsoft® Windows® Server 2003 Resource Kit* (or see the *Server Management Guide* on the Web at <http://www.microsoft.com/reskit>).

**Use third-party disk configuration tools** Some third-party disk-imaging programs and disk management programs provide a bootable floppy disk or CD that allows you to partition and format a hard disk before you copy the disk image onto the destination computer. If you use a third-party program to partition or format a disk, be sure that the third-party program creates partitions that are compatible with NTFS 3.1, which is the version of NTFS that is used in the Windows XP Professional and Windows Server 2003 operating systems.



**Use the Windows Preinstallation Environment** You can start a destination computer by using a Windows Preinstallation Environment (Windows PE) CD, and then using the **diskpart** command to partition a disk and the **format** command to format a disk. Windows PE is a bootable operating system that provides limited operating system functionality for performing preinstallation tasks. Windows PE is only available if you have purchased Enterprise Agreement 6.0, Enterprise Subscription Agreement 6.0, or Select License 6.0 with Software Assurance (SA). For more information about Windows PE and Windows PE licensing plans, see the Windows Preinstallation Environment link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>. For more information about the **diskpart** command, see “DiskPart Scripting” in the *Microsoft Windows Corporate Deployment Tools User’s Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.

Each method of configuring disk settings has advantages and disadvantages. You need to determine which method is better suited to your organization and your deployment needs.

## Components of a Disk Configuration Plan

After you determine which method to use to configure disk settings, you need to create your disk configuration plan. At a minimum, your disk configuration plan must identify:

- **Disk configuration settings.** Disk configuration settings include the number of partitions, partition sizes, and file system formats. Disk configuration settings are based on several factors, including disk sizes, disk types, backup capabilities, and user needs. Analyze these factors in your disk configuration plan to determine the right disk configuration for your organization.
- **Procedures for configuring disk settings.** Your disk configuration plan must describe every step of the disk configuration process, including how to start a destination computer and how to run the partitioning or formatting tools.
- **Tools that you use to configure disk settings.** Disk configuration tools include the **format**, **fdisk**, and **diskpart** commands. Your disk configuration plan must describe all the tools you will use to configure disk settings, including the tools you will use to start a destination computer and to partition, format, and check a disk.



### Important

You need to rewrite the disk signature if your destination computer’s partition is smaller than the new image partition you are copying. Failure to rewrite the disk signature in this case can prevent you from copying a disk image to a disk drive. For example, if you have a target computer with two 5 GB partitions and you need to install an image that is 8 GB, you will need to rewrite the disk signature. You can accomplish this with some disk-imaging programs, but Microsoft does not support doing so. You can also accomplish it with **fdisk -mbr**. The **format** command will not rewrite the disk signature.

# Designing Automated Setup Tasks

You can automate the following installation tasks after a disk image is copied onto a destination computer:

- **Mini-Setup.** You can automate Mini-Setup, which is a subset of Windows Setup, by using Sysprep.inf. Mini-Setup runs automatically after you copy a disk image onto a destination computer and an end user starts the destination computer. The primary role of Mini-Setup is to gather user-specific information, and detect and install hardware.
- **Software installation and configuration.** You can automatically install and configure client and server applications. You can also install and configure Windows components.
- **Hardware installation and configuration.** You can automatically update device drivers and configure device settings.
- **Computer configuration.** You can automatically configure computer settings, such as network protocols, display settings, and system services. You can also configure server roles; for example, you can promote servers to domain controllers.

Try to automate as many installation tasks as possible. By automating installation tasks, you can:

- Lower the number of errors caused by technicians, administrators, and end users during your deployment.
- Ensure consistency throughout your organization, which reduces support costs after you complete your deployment.
- Increase productivity by requiring little or no end-user interaction during your deployment.
- Update or modify your installation process without having to educate or retrain end users, technicians, or administrators.

To automate installation tasks, you need to use several types of configuration files, including information (.inf) files, answer (.txt) files, and initialization (.ini) files. Configuration files contain information that is used to answer end-user prompts and configure computer settings before, during, and after Mini-Setup. Configuration files can also contain instructions for running programs, scripts, or commands before, during, and after Mini-Setup. The following configuration files are used to automate installation tasks.

**Sysprep.inf** You can use this file to automate Mini-Setup, configure computer settings, and automatically run programs, scripts, or commands during and after Mini-Setup. When you copy a disk image onto a destination computer, the destination computer automatically searches for Sysprep.inf the first time it is started.

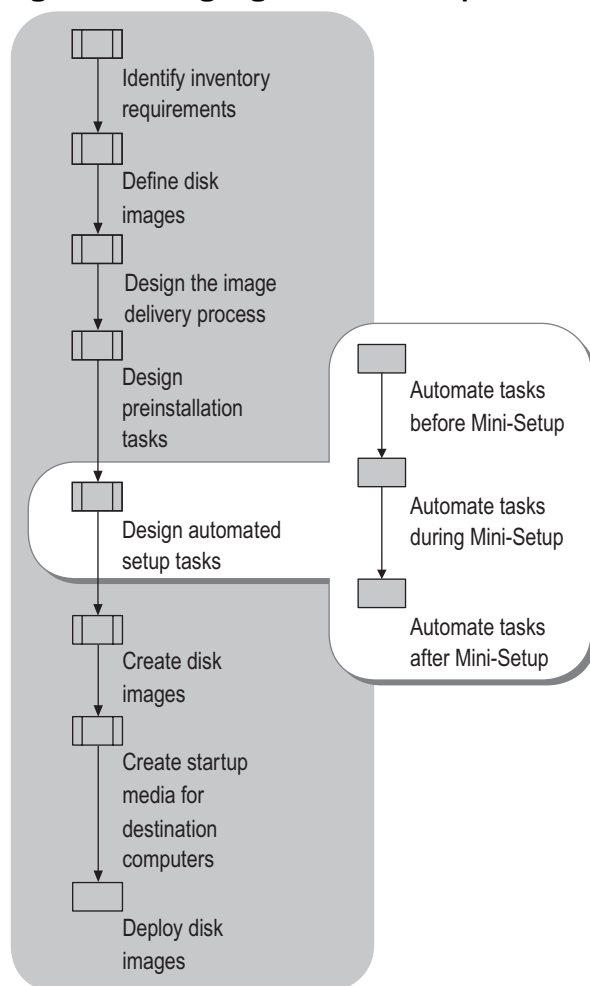
**Cmdlines.txt** You can use this file to automatically run programs, scripts, or commands during Mini-Setup. You must configure the InstallFilePath parameter in Sysprep.inf to use the Cmdlines.txt file.

**Unattend.txt** You can use this file to automate a program so that no user input is required. For example, an Unattend.txt file can be used with Dcpromo.exe (the Active Directory Installation Wizard) to automatically configure a server as a domain controller.

**Winbom.ini** You can use this file to install software, update device drivers, and configure operating system settings after you copy a disk image onto a destination computer but before you prepare the computer for final delivery to an end user. You can also use this file to run auditing scripts or programs, which can help you identify device errors and verify that your applications and drivers are installed properly.

Figure 3.6 shows the process you need to follow to design an automated image-based installation.

**Figure 3.6 Designing Automated Setup Tasks**



## Automating Tasks Before Mini-Setup

You can automate some installation and configuration tasks before Mini-Setup runs by using a special Sysprep feature known as *Factory mode*. Factory mode is a network-enabled state that uses an answer file to automate installation and configuration tasks before you prepare the computer for final delivery to an end user. Factory mode is commonly used in a manufacturing environment where every computer requires some customization prior to final delivery to an end user; however, it is also useful for corporate deployments. Use Factory mode if you want to customize individual computers or groups of computers after you have copied a disk image onto a destination computer but before Mini-Setup runs.

To automate installation tasks in Factory mode, you need to configure a Winbom.ini file (short for “Windows bill of materials”). Winbom.ini is the answer file for Factory mode. Using Winbom.ini is a completely automated process. You prepare a master computer by using the **-factory** parameter with Sysprep, and then create a disk image of the master computer. You then copy the image onto a destination computer. The first time the destination computer starts, it starts in Factory mode and automatically searches for Winbom.ini. The computer then automatically performs the installation and configuration tasks you specified in Winbom.ini. When the destination computer finishes all of the tasks listed in Winbom.ini, you must run Sysprep with the **-reseal** parameter, which prepares the computer for delivery to an end user. To do this, use the Reseal and ResealMode entries in the [Factory] section of Winbom.ini. Factory.exe must be present in the Sysprep\I386\SOEM\$ folder with Sysprep.exe and Setupcl.exe in order for Factory mode to work.



### Note

You cannot manually install and configure software and system components when a computer is in Factory mode. You must use a Winbom.ini file to install and configure software and system components when a computer is in Factory mode.

For corporate deployments, where you typically do not need to create a unique Winbom.ini file for every computer, you can create Winbom.ini files manually by using a text editor.

Use Factory mode and a Winbom.ini file to automate installation tasks before Mini-Setup if you need:

- **Network connectivity.** You can access resources in shared folders, such as data files, device drivers, and applications.
- **Choice of security context.** You can choose a user account under which to run automated installation tasks.

- **Staged installation support.** You can stage the installation of software, which is the fastest method of installing and configuring applications after you copy a disk image onto a destination computer. For more information about staging the installation of applications, see “Preinstalling Applications” in the *Microsoft Windows Corporate Deployment Tools User’s Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.
- **Windows Installer support.** You can use Windows Installer (.msi) packages to install programs.
- **Disk configuration support.** You can create partitions and format disks on a destination computer, but only if you use Factory mode with the Windows Preinstallation Environment.
- **Synchronous and asynchronous program execution.** You can run programs, scripts, and batch files synchronously by using the [OEMRunOnce] section of Winbom.ini, or asynchronously by using the [OEMRun] section of Winbom.ini. During *synchronous execution*, each program does not run until the previous program finishes running. During *asynchronous execution*, programs start one after the other without waiting for the previous program to finish running.
- **Faster uptime for end users.** You can reduce the number of installation tasks that need to be performed after a computer is delivered to an end user.
- **Auditing support.** You can perform auditing tasks after a destination computer has been started in Factory mode.
- **Device driver installation support.** You can use the [PnPDrivers] and [PnPDriverUpdate] sections of Winbom.ini to connect to a server and download device drivers. By comparison, when you use the [OEMPnPDriversPath] section of Sysprep.inf, you can only copy device drivers from the local hard disk.

There are some limitations to automating installation tasks before Mini-Setup runs. You cannot use Factory mode and a Winbom.ini file to do the following:

- Perform installation and configuration tasks that publish information in Active Directory.
- Install and configure Cluster service and domain controllers.
- Perform installation and configuration tasks that rely on the computer name or the computer’s SIDs.

To design automated installation tasks that occur before Mini-Setup, you must identify:

- The installation tasks you want to automate.
- The configuration files you need to use.
- The settings you need to configure for each configuration file.

### Identifying Automated Installation Tasks You Can Perform Before Mini-Setup

You can use each copy of the “Disk Image Worksheet” (ACISYS\_1.doc) to identify the installation tasks you need to perform after each of your disk images is copied onto a destination computer. If you have not created a worksheet for each of your disk images, identify the installation and configuration tasks that need to be performed after each of your disk images is copied onto a destination computer.

Next, use Table 3.5 to determine which installation tasks to automate before Mini-Setup. Try to automate as many installation tasks as possible.

**Table 3.5 Installation Tasks You Can Automate Before Mini-Setup**

Installation Task	Comments
Install Windows components	These include all Windows components listed in Add or Remove Programs in Control Panel, such as accessories, games, media services, and networking services.
Install and configure software	This includes Windows Installer (.msi) packages as well as staged software. Software installation must run in quiet mode, which means the installation must be fully automated and cannot rely on user interaction. Usually, when you run an installation program in quiet mode, you must provide an answer file.
Configure computer settings	These include power management and display settings.
Run programs, scripts, and batch files	Programs, scripts, and batch files must be fully automated and cannot rely on user interaction, which means you must provide an answer file for any programs, scripts, or batch files you are running, and you must be able to run the programs, scripts, or batch files in quiet mode.
Update device drivers	Device driver files are copied onto the destination computer and the device driver location is added to the device path, which is stored in the registry. (The device path tells the Plug and Play module where drivers are stored). The Plug and Play feature installs the drivers the next time the computer starts.
Configure shell settings	These include desktop themes, Windows Messenger, and the appearance of the Start menu.
Enable an Internet connection firewall	Enables the firewall feature in Windows XP and Windows Server 2003.

**(continued)**

**Table 3.5 Installation Tasks You Can Automate Before Mini-Setup (continued)**

Installation Task	Comments
Configure the list of most frequently opened or accessed applications	The list of most frequently opened or accessed applications can be configured for specific users.
Update registry and file settings	Uses directives based on Windows .inf file processing standards. For information about .inf file sections and directives, see the Driver Development Kits link on the Web Resources page at <a href="http://www.microsoft.com/windows/reskits/webresources">http://www.microsoft.com/windows/reskits/webresources</a> .
Configure user accounts	This includes user name, .NET Passport, password, and description settings.
Update files	This includes renaming, deleting, or copying files in addition to updating the contents of .inf and .ini files.
Extend a primary partition	Extends the primary partition that the Windows operating system is installed on.
Configure Internet Explorer Enhanced Security Configuration	This includes configuring Internet Explorer Enhanced Security Configuration for members of the User and Guests groups, and the Administrators group.*

\* For more information about Internet Explorer Enhanced Security Configuration settings, see "Internet Explorer Enhanced Security Configuration" in Help and Support Center for Windows Server 2003. For more information about answer file settings related to Internet Explorer Enhanced Security Configuration, see the Readme.txt file in Deploy.cab. Deploy.cab is in the Support folder on the Windows Server 2003 operating system CD.

You can perform other automated installation tasks with a Winbom.ini file if you are using Factory mode with the Windows Preinstallation Environment. For more information about these tasks, see the *Microsoft Windows Corporate Deployment Tools User's Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.

## Identifying Configuration Files to Use Before Mini-Setup

You might have to configure several answer files or configuration files if you automate installation tasks before Mini-Setup. Table 3.6 describes these answer files and configuration files, and explains where you need to save them.

**Table 3.6 Configuration Files Used to Automate Tasks Before Mini-Setup**

Configuration File	Description	Where to Save the Configuration File
Winbom.ini	Answer file for Factory mode.	Any of the following locations: <ul style="list-style-type: none"> <li>The root of all removable media drives, including CD-ROM drives and floppy disk drives.</li> <li>The same location as Factory.exe (usually the <i>systemdrive</i>\Sysprep folder).</li> <li>The root of <i>systemdrive</i>.</li> </ul>
<i>filename.txt</i> *	Answer file for programs or scripts that run during Factory mode. This includes answer files for software installation (setup) programs.	Any location you specify in the [OEMRun] or [OEMRunOnce] section of Winbom.ini.
<i>filename.theme</i> *	Configuration file for desktop themes.	Any location you specify in the [Shell] section of Winbom.ini.

\* Where *filename* can be any valid file name you choose.

For more information about how to configure an answer file for a program or script, see the documentation for the program or script. For more information about configuring a .theme file, see the Core Software Development Kit (SDK). To download the Core SDK, see the Microsoft Platform SDK link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

## Identifying Configuration File Settings for Winbom.ini

Use Table 3.7 to match an installation task with a specific section in a Winbom.ini file.

**Table 3.7 Installation Tasks and Corresponding Winbom.ini Section Names**

To Automate This Task	Configure These Sections of Winbom.ini
Install Windows components	[Components]
Install and configure software	[OEMRun], [OEMRunOnce]
Configure computer settings	[ComputerSettings]
Run programs, scripts, and batch files	[OEMRun], [OEMRunOnce]
Update device drivers	[PnPDrivers], [PnPDriversUpdate]

(continued)



**Table 3.7 Installation Tasks and Corresponding Winbom.ini Section Names (continued)**

To Automate This Task	Configure These Sections of Winbom.ini
Configure shell settings	[Shell]
Enable an Internet connection firewall	[SetupHomenet]
Configure the list of most frequently used applications	[StartMenuMFUlist]
Update registry and file settings	[UpdateSystem]
Configure user accounts	[UserAccounts]
Update files	[UpdateSystem]
Extend a primary partition	[ComputerSettings]

For more information about specific configuration file settings, including procedural and reference information about creating, formatting, and configuring a Winbom.ini file, see the *Microsoft Windows Corporate Deployment Tools User's Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.

## Automating Tasks During Mini-Setup

You can automatically update device drivers and configure user preferences and computer settings during Mini-Setup by using a Sysprep.inf file. Sysprep.inf is most commonly used as the answer file for Mini-Setup, but you can use it to perform other automated tasks during Mini-Setup. For example, if you use Sysprep.inf in conjunction with a Cmdlines.txt file, you can install software and run programs, scripts, and batch files just after Mini-Setup is finished but before a destination computer shuts down or restarts.

When you prepare a disk image with Sysprep and then copy the image onto a destination computer, the destination computer automatically searches for Sysprep.inf the first time it starts and automatically performs the installation and configuration tasks you specify in Sysprep.inf. When the destination computer finishes all of the tasks listed in Sysprep.inf, it restarts and is ready for use by an end user (unless there are automated tasks that need to be performed after Mini-Setup runs — in that case, the tasks are performed, the computer restarts, and then it is ready for use by an end-user).

Use a Sysprep.inf file to automate installation tasks during Mini-Setup if you need:

- **Automated Mini-Setup.** You can automate end-user prompts during Mini-Setup, which reduces the amount of end user interaction.
- **Page file regeneration.** You can delete and recreate the page file on the disk image, which is useful if the amount of RAM on the destination computer is different from the amount of RAM that was on the master computer.

- **Mass storage controller support.** You can predefine driver information for mass storage controllers so that Windows loads the correct mass storage controller driver on a destination computer.
- **Cmdlines.txt support.** You can use this file to install programs or run programs, scripts, and batch files when Mini-Setup is finished but before the computer restarts. All tasks listed in Cmdlines.txt run under the Local System security account because there is no logged-on user.

Automating tasks during Mini-Setup has some limitations. You cannot automate tasks during Mini-Setup if:

- You need network connectivity. You cannot access network resources, such as shared folders, during Mini-Setup. This is also true for any tasks you automate by using a Cmdlines.txt file.
- You need to perform a task under a specific user account. All tasks are performed under the Local System security account during Mini-Setup. This is also true for any tasks you automate by using a Cmdlines.txt file.
- You want to install software by using Windows Installer packages. You cannot use the Cmdlines.txt file to install .msi packages.

You can create a Sysprep.inf file either by using Setup Manager or by using a text editor such as Notepad. Setup Manager steps you through the Mini-Setup process and records your answers in a Sysprep.inf file. Setup Manager is included in the Deploy.cab file in the Support folder on the *Windows Server 2003* operating system CD. For more information about using Setup Manager, see the *Microsoft Windows Corporate Deployment Tools User's Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.

To design automated installation tasks that occur during Mini-Setup, you must identify:

- The installation tasks you want to automate.
- The configuration files you need to use.
- The settings you need to configure for each configuration file.

### **Identifying Automated Installation Tasks You Can Perform During Mini-Setup**

You can use each copy of the “Disk Image Worksheet” (ACISYS\_1.doc) to identify the installation tasks you need to perform after each of your disk images is copied onto a destination computer. If you have not created a worksheet for each of your disk images, identify the installation and configuration tasks that need to be performed after each of your disk images is copied onto a destination computer.

Next, use Table 3.8 to determine which installation tasks to automate during Mini-Setup. If possible, automate tasks before Mini-Setup by using Factory mode and a Winbom.ini file.

**Table 3.8 Installation Tasks You Can Automate During Mini-Setup**

Installation Task	Comments
Extend a primary partition	Extends the primary partition that the Windows operating system is installed on. This task is performed during the Mini-Setup phase of installation, but just before Mini-Setup runs.
Update device drivers and device path	Runs Plug and Play at the end of Mini-Setup to re-enumerate all the installed drivers and install any updated drivers that are found in the device path. The device path tells the Plug and Play module where device drivers are located, and is stored in the registry. You can also change the device path.
Regenerate a page file	Deletes and regenerates a page file based on the amount of RAM in the destination computer. This task is performed during the Mini-Setup phase of installation, but just before Mini-Setup runs.
Install drivers for mass storage controllers	This task is performed during the Mini-Setup phase of installation, but just before Mini-Setup runs.
Configure user settings	These settings include computer name, user name, organization name, and product key. If you automate this task, end users are not prompted for this information during Mini-Setup.
Configure regional options	These options include locale and language settings. If you automate this task, end users are not prompted for this information during Mini-Setup.
Set date and time	If you automate this task, end users are not prompted for this information during Mini-Setup.
Set server licensing mode	If you automate this task, end users are not prompted for this information during Mini-Setup.
Configure display settings	These settings include color depth, resolution, and refresh rate. If you automate this task, end users are not prompted for this information during Mini-Setup.
Configure telephony settings	These include area code, country code, dial tone type, and number to dial for an outside line. If you automate this task, end users are not prompted for this information during Mini-Setup.

*(continued)*

**Table 3.8 Installation Tasks You Can Automate During Mini-Setup (continued)**

Installation Task	Comments
Configure computer settings	These include computer name, organizational unit membership, domain or workgroup membership, and administrator password. If you automate this task, end users are not prompted for this information during Mini-Setup.
Configure network settings	These include installation of optional networking components and configuration of network services, protocols, and network adapters. If you automate this task, end users are not prompted for this information during Mini-Setup.
Install software	If you use Cmdlines.txt to install software, you cannot use .msi packages and you cannot access network resources. In addition, installation tasks are run under the Local System security account because there is no logged-on user.
Run programs, scripts, and batch files	You cannot access network resources if programs, scripts, or batch files are run with Cmdlines.txt. In addition, programs, scripts, and batch files are run under the Local System security account because there is no logged-on user.

### Identifying Configuration Files to Use During Mini-Setup

You might have to configure several answer files or configuration files if you automate installation tasks during Mini-Setup. Table 3.9 describes these answer files and configuration files, and explains where you need to save them.

**Table 3.9 Configuration Files Used to Automate Tasks During Mini-Setup**

Configuration File	Description	Where to Save the Configuration File
Sysprep.inf	Primarily the answer file for Mini-Setup, but can also be used to configure computer settings.	Must be saved in the same location as Sysprep.exe and Setupcl.exe, which are in the <i>systemdrive</i> \Sysprep folder on the destination computer.
Cmdlines.txt	Configuration file for running programs, scripts, or batch files during Mini-Setup.	Must exist in the <i>systemdrive</i> \Sysprep\%OEM\$ folder on the destination computer's hard disk.
<i>filename.txt</i> *	Answer file for programs or scripts that run during Mini-Setup. This includes answer files for software installation (setup) programs.	Same location as the program or script that you need to run without user intervention during Mini-Setup.

\* Where *filename* can be any valid file name you choose.

You can use different Sysprep.inf files with a single disk image by copying Sysprep.inf to the *systemdrive\Sysprep* folder after you copy the disk image to a destination computer. The easiest way to do this is to start the destination computer in Factory mode, and then copy the appropriate Sysprep.inf file from a shared folder to the *systemdrive\Sysprep* folder. You can also use a disk-imaging application to copy files onto a disk image after the disk image has been created, although not all disk-imaging programs provide this functionality.



#### Note

You can also save Sysprep.inf on a floppy disk with Sysprep.exe and Setupcl.exe; however, the floppy disk controller on the master computer must be identical to the floppy disk controller on the destination computer. If the floppy disk controllers are different, the Setup program will not find the floppy disk controller on the destination computer, and the automated tasks and settings specified in Sysprep.inf will fail.

For more information about using Sysprep.inf and Cmdlines.txt files, see the *Microsoft Windows Corporate Deployment Tools User's Guide* (Deploy.chm), which is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD. For more information about how to configure an answer file for a program or script, see the documentation for the program or script.

### Identifying Configuration File Settings for Sysprep.inf

Use Table 3.10 to match an installation task with a specific section and parameter in a Sysprep.inf file.

**Table 3.10 Installation Tasks and Corresponding Sysprep.inf Section Names**

To Automate This Task	Configure These Sections in Sysprep.inf
Extend a primary partition	[Unattended]
Update device drivers and change device path	[Unattended]
Regenerate a page file	[Unattended]
Install drivers for mass storage controllers	[Sysprep] and [SysprepMassStorage]
Configure user settings	[UserData]
Configure regional options	[GuiUnattended] and [RegionalSettings]
Set date and time	[GuiUnattended]
Set server licensing mode	[LicenseFilePrintData]
Configure display settings	[Display]
Configure telephony settings	[TapiLocation]

(continued)

**Table 3.10 Installation Tasks and Corresponding Sysprep.inf Section Names (continued)**

To Automate This Task	Configure These Sections in Sysprep.inf
Configure computer settings	[Networking] and [Identification]
Configure network settings	[Networking]
Install software	[GuiRunOnce]
Run programs, scripts, and batch files.	[GuiRunOnce]

**Note**

You can also use the [GuiRunOnce] section in a Sysprep.inf file to install software and run programs, scripts, and batch files. All tasks that are listed in the [GuiRunOnce] section occur after Mini-Setup finishes and the computer restarts. For more information about the [GuiRunOnce] section, see “Automating Tasks After Mini-Setup” later in this chapter.

---

## Automating Tasks After Mini-Setup

You can automatically install software and run commands, programs, scripts, and batch files after Mini-Setup runs and the computer restarts by using the [GuiRunOnce] section in Sysprep.inf. All of the tasks listed in the [GuiRunOnce] section of a Sysprep.inf file are stored in the following registry subkey:

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Runonce

When a computer is started for the first time after Mini-Setup, the commands listed in the [GuiRunOnce] section are read from the registry and executed.

Automate tasks by using the [GuiRunOnce] section in Sysprep.inf if you need:

- **Choice of security context.** You can install software and run programs, scripts, and batch files under the context of an end user or a local Administrator account.
- **Network access.** You can access network resources, such as shared folders and drives.
- **Server configuration support.** You can install Cluster service and configure domain controllers.
- **Active Directory support.** You can access Active Directory, depending on the security context of the logged-on user.

On the other hand, automating tasks by using the [GuiRunOnce] section in Sysprep.inf has one key disadvantage: longer startup time for end users. End users must wait for the tasks specified in the [GuiRunOnce] section to run before they can access their computers.

You can configure the [GuiRunOnce] section in a Sysprep.inf file either by using Setup Manager or by using a text editor such as Notepad. Setup Manager prompts you for commands, programs, scripts, or batch files that you want to run after Mini-Setup runs and a computer restarts. Your answers are saved in the [GuiRunOnce] section of a Sysprep.inf file. Setup Manager is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD. For more information about using Setup Manager, see the *Microsoft Windows Corporate Deployment Tools User's Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.

To design automated installation tasks that occur after Mini-Setup, you must identify:

- The installation tasks you want to automate.
- The configuration files you need to use.
- The settings you need to configure for each configuration file.

### Identifying Automated Installation Tasks You Can Perform After Mini-Setup

You can use each copy of the “Disk Imaging Worksheet” (ACISYS\_1.doc) to identify the installation tasks you need to perform after each of your disk images is copied onto a destination computer. If you have not created a worksheet for each of your disk images, identify the installation and configuration tasks that need to be performed after each of your disk images is copied onto a destination computer.

Next, use Table 3.11 to determine which installation tasks to automate after Mini-Setup. If possible, try to automate tasks before Mini-Setup by using Factory mode and a Winbom.ini file.

**Table 3.11 Installation Tasks You Can Automate After Mini-Setup**

Installation Task	Comments
Install software	Software installation tasks are run under either the end user or local Administrator account.
Run commands, programs, scripts, and batch files	Commands, programs, scripts, and batch files are run under the security context of the end user or the local Administrator account.

## Identifying Configuration Files to Use After Mini-Setup

You might have to configure several answer files or configuration files if you automate installation tasks after Mini-Setup. Table 3.12 describes these answer files and configuration files, and explains where you need to save them.

**Table 3.12 Configuration Files Used to Automate Tasks After Mini-Setup**

Configuration File	Description	Where to Save the Configuration File
Sysprep.inf	Primarily the answer file for Mini-Setup, but can also be used to run programs, scripts, or batch files after Mini-Setup runs and a destination computer restarts. To do this, you must include the programs, scripts, or batch files in the [GuiRunOnce] section of Sysprep.inf.	Must be saved in the same location as Sysprep.exe and Setupcl.exe, which are in the <i>systemdrive</i> \Sysprep folder on the destination computer.
<i>filename.txt</i> *	Answer file for programs or scripts that run after Mini-Setup and a computer restarts. This includes answer files for software installation (setup) programs.	Same location as the program or script that you need to run without user intervention after Mini-Setup.

\* Where *filename* can be any valid file name you choose.

You can use different Sysprep.inf files with a single disk image by copying Sysprep.inf to the *systemdrive*\Sysprep folder after you copy the disk image to a destination computer. The easiest way to do this is to start the destination computer in Factory mode, and then copy the appropriate Sysprep.inf file from a shared folder to the *systemdrive*\Sysprep folder. You can also use a disk-imaging application to copy files onto a disk image after the disk image has been created, although not all disk-imaging programs provide this functionality.



### Note

You can also save Sysprep.inf on a floppy disk with Sysprep.exe and Setupcl.exe; however, the floppy disk controller on the master computer must be identical to the floppy disk controller on the destination computer. If the floppy disk controllers are different, the Setup program will not find the floppy disk controller on the destination computer, and the automated tasks and settings specified in Sysprep.inf will fail.

For more information about using Sysprep.inf and Cmdlines.txt files, see the *Microsoft Windows Corporate Deployment Tools User's Guide* (Deploy.chm), which is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD. For more information about how to configure an answer file for a program or script, see the documentation for the program or script.



### Identifying Configuration File Settings to Use After Mini-Setup

To run programs, scripts, or batch files after Mini-Setup runs and a destination computer restarts, you must use the [GuiRunOnce] section of Sysprep.inf. Programs, scripts, and batch files that are run using the [GuiRunOnce] section run in the context of the currently logged-on end user. If the end user does not have the necessary user rights to run the program, script, or batch file completely, the application fails. Because programs, scripts, and batch files are run in the context of a logged-on end user rather than as a service, the registry entries that the application creates are written for the current end user rather than the default user. (Default user registry settings are propagated to new end users.) If you want any settings and updates to show specifically for the logged-on end user only, using the [GuiRunOnce] section is appropriate. Otherwise, you can use Cmdlines.txt to run applications because it runs programs, scripts, and batch files under the context of the Local System security account.

For more information about configuring the [GuiRunOnce] section in Sysprep.inf, see the *Microsoft Windows Corporate Deployment Tools User's Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.

---

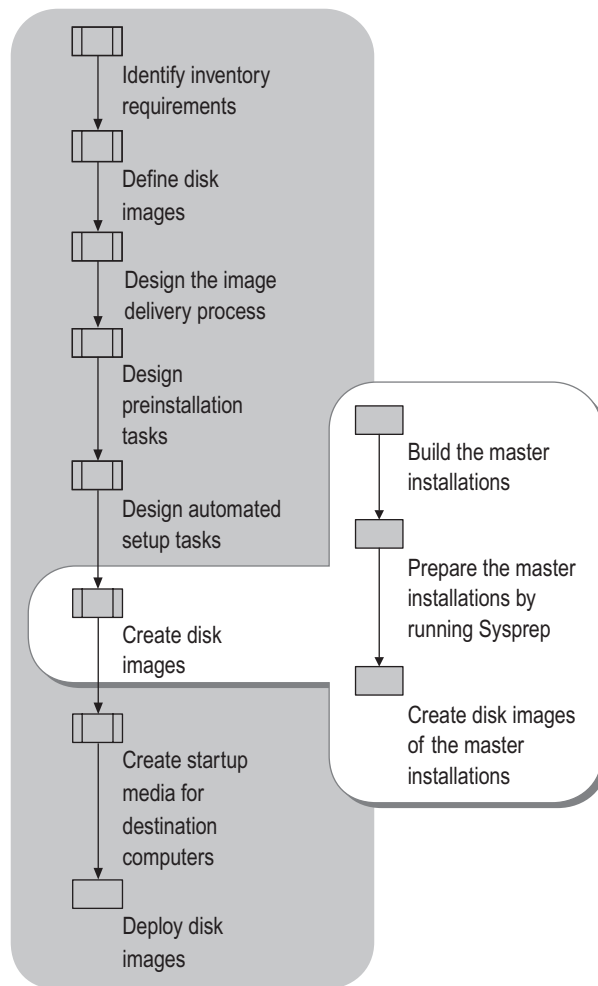
## Creating Disk Images

Creating disk images is a straightforward process that involves three key tasks:

- Build a master installation for each of your disk images. A master installation is built on a master computer. Building a master installation includes installing and configuring the operating system and any software you want to include on your disk image.
- Prepare each master installation by using Sysprep. This includes configuring and running Sysprep on each master computer.
- Create a disk image of each master installation by using the disk-imaging program. This includes saving each disk image to a permanent storage location.

Figure 3.7 shows the process you must follow to create disk images. None of the steps are optional: you must perform each step in the order shown.

**Figure 3.7 Creating Disk Images**



# Building Master Installations

To build a master installation, you need to configure disk settings, install the operating system and software, and configure operating system and software settings. You can automate some or all of these tasks, or you can perform them manually on each of your master computers.

## Configuring Disk Settings on a Master Installation

To configure disk settings on a master computer, you need to perform the following tasks.

### Determine minimum disk size

Use the “Disk Image Worksheet” (ACISYS\_1.doc) or your hardware inventory to determine the minimum available disk space for each disk image. The minimum available disk space for a disk image will be either the smallest hard disk or the smallest system partition among the destination computers.

### Determine partition size and file system format

Use the job aid “Disk Image Worksheet” (ACISYS\_1.doc) to determine the partition size and file system format you want to use on each disk image. The size of the system partition on each master installation must be equal to or less than the minimum hard disk or partition size on your destination computers. If you create a partition on the master installation that is smaller than the minimum hard disk or partition size on your destination computers, you can use the `ExtendOemPartition` parameter in `Sysprep.inf` to extend the partition on the destination computer after you copy the disk image onto it. There are several reasons to create a master installation on a partition that is smaller than the minimum hard disk or partition size on your destination computers:

- You reduce installation time if you are distributing disk images across a network.
- You reduce the number of CDs or DVDs you need for each disk image if you are distributing disk images on media.
- You reduce the amount of file server space you need to store your disk images.
- You reduce the amount of time it takes to create disk images.

### Format and partition the hard disk on the master computer

Use Microsoft tools, such as the **fdisk**, **diskpart**, and **format** commands, to create and format partitions. Also, be sure to create your master installation on drive C.

## Installing and Configuring a Master Installation

Use the “Disk Image Worksheet” to determine the operating system and software you need to install, and the settings you need to configure, for each of your master installations. For a master installation, you can configure the operating system and software using one of three methods.

### Manual installation and configuration method

You can manually install the operating system by using Windows Setup, and then manually install software and configure system settings. There are two ways you can do this:

- Start the master computer by using the Windows Server 2003 operating system CD. Windows Setup will start automatically. When you finish installing the operating system, you can then install and configure software applications.
- Start the master computer by using an MS-DOS startup disk, and then start Windows Setup by running Winnt.exe, which is located in the I386 folder on the operating system CD. When you finish installing the operating system, you can then install and configure software applications.

### Semi-automated installation and configuration method

You can use an answer file to automate Windows Setup, and then manually install and configure software. This automated method of installing the operating system is known as unattended installation. You can perform an unattended installation by starting the master computer with an operating system CD, and then automating Windows Setup by using a Winnt.sif answer file. You can also perform an unattended installation by starting the master computer with an MS-DOS startup disk, and then automating Windows Setup by using an Unattend.txt answer file.

### Fully automated installation and configuration method

To fully automate the installation and configuration of the operating system and software, you can use answer files in conjunction with configuration sets that reside on a distribution share. A *configuration set* contains device drivers, software files, answer files, and configuration settings that are required to build a master installation. A *distribution share* is a shared folder that contains all of your configuration sets. You can use Setup Manager to create configuration sets.

Table 3.13 compares the three methods of building master installations.

**Table 3.13 How Manual and Automated Methods of Building Master Installations Differ**

Benefit/Requirement	Manual Method	Semi-automated Method	Automated Method
Stores master installation files in a central location.	No. Master installation files, such as device drivers and answer files, are transferred directly from operating system CDs, file shares, and floppy disks to the master computers.	No. Master installation files, such as device drivers and answer files, are transferred directly from operating system CDs, file shares, and floppy disks to the master computers.	Yes. Master installation files are transferred from operating system CDs, file shares, and floppy disks to a centralized distribution share.
Requires a fast network connection between the file server and master computers.	No. Network connectivity is only necessary if you need to access installation files that are not on a CD or floppy disk.	No. Network connectivity is only necessary if you need to access installation files that are not on a CD or floppy disk.	Yes. Network connectivity is necessary to transfer installation files from the distribution share on a file server to a master computer.
Simplifies updating and modifying disk images.	No. Each master installation must be updated or modified individually before new disk images can be created.	Yes. Master installations can be updated by modifying answer files, and then automatically installed on master computers before new disk images are created.	Yes. Master installations are updated at a single location and then automatically installed on master computers before new disk images are created.
Simplifies testing.	No. Errors must be fixed on each master computer.	Yes. Errors can be fixed in answer files and then each master computer can be automatically updated.	Yes. Errors can be fixed on the distribution share and then each master computer can be automatically updated.

(continued)

**Table 3.13 How Manual and Automated Methods of Building Master Installations Differ (continued)**

Benefit/Requirement	Manual Method	Semi-automated Method	Automated Method
Requires record-keeping to track installation and configuration information for each disk image.	Yes. You must keep a record of the installation and configuration procedures you performed for each disk image.	Some. The answer files track operating system installation and configuration information, but you still need to record information about the software that is installed on each disk image.	No. The answer files in each configuration set provide installation and configuration information for each disk image.
Complements unattended installations.	No. Manually installing and configuring master installations does not affect your unattended installations.	Somewhat. You can use the answer files to perform your unattended installations.	Yes. The distribution share you use to create your master installations can be used to perform your unattended installations.
Ensures consistency every time you make a change to a master installation.	No. Changes are made individually to each master installation by a technician or administrator, which increases the potential for inconsistency and errors.	Somewhat. Changes to the operating system are made through answer files, which lessens the potential for errors; however, changes to software are made individually to each master installation by a technician or administrator, which increases the potential for inconsistency and errors.	Yes. Changes are made to configuration sets on a centralized distribution share, which lessens the potential for inconsistency and errors.

You can use the following guidelines to determine which method to use to build your master installations.

Choose manual installation and configuration if any of the following are true:

- You are creating no more than three disk images.
- You seldom upgrade computers and you seldom perform unattended installations.
- You seldom update the configuration of your disk images.
- You have limited network bandwidth in your organization.
- You have limited file server capacity in your organization.

Choose semi-automated or automated installation and configuration if any of the following are true:

- You are creating more than three disk images.
- You frequently upgrade computers or perform unattended installations.
- You frequently change the configuration of your disk images.

For more information about installing and configuring a master installation, and for more information about using Setup Manager to create configuration sets and distribution shares, see the *Microsoft Windows Corporate Deployment Tools User's Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD. For more information about answer files, distribution shares, and unattended and automated installations, see “Designing Unattended Installations” in this book.



### Important

You must perform all installation and configuration tasks under the local Administrator account on your master installation. This ensures that all configuration settings are stored in the same user profile and that all global configuration settings are stored in the Default User or All Users user profiles.

## Preparing Master Installations by Running Sysprep

Before you can create your disk images, you must prepare each of your master installations. The preparation process cleans up, configures, audits, and prepares a master installation so an image of its disk can be created and then distributed to destination computers.

To prepare your master installations for imaging:

- Identify the cleanup, configuration, and auditing tasks you need to perform.
- Choose the settings you need to configure when you run Sysprep.

---

### Identifying Cleanup, Configuration, and Auditing Tasks

You perform cleanup, configuration, and auditing tasks on each of your master installations before you run Sysprep. For a typical image-based installation, you perform the following cleanup, configuration, and auditing tasks in the order in which they are presented. Perform the following tasks under the local Administrator account, except where noted otherwise.

1. Delete files and folders that you do not want end users to see, such as:
  - Files and folders that you used to build the master installation, such as tools, documents, and scripts.
  - Temporary Internet files, including cookies.
  - Temporary user files, which can include items in *systemroot*\Temp, *systemdrive*\Temp, and the folder used by the TEMP environment variable.
  - Files and folders in the Recycle Bin.
  - Files and folders in My Documents.

2. Create a folder for the Sysprep tool and configuration files.

To do this, create a folder named Sysprep in the root directory of your master installation (for example, C:\Sysprep). Next, extract the Sysprep tool from Deploy.cab, which is located in the Support folder on the Windows Server 2003 operating system CD and the Windows XP Professional operating system CD. The Sysprep tool comprises three files: Sysprep.exe, Setupcl.exe, and Factory.exe. The Sysprep folder is deleted when a destination computer is restarted after Mini-Setup.

3. Remove the master computer from the domain and add it to a workgroup.

Sysprep cannot completely finish running if the master computer is joined to a domain. If the master computer is joined to a domain, Sysprep will automatically remove it from the domain; however, the preferred method is to remove the master computer from the domain before you run Sysprep. Do not restart the computer when prompted to do so.



#### 4. Run auditing and diagnostic tools.

Run all auditing and diagnostic tools, such as Disk Defragmenter, Check Disk, and virus detection tools. Be sure to delete any temporary files created by the auditing and diagnostic tools. Also run the Microsoft Baseline Security Analyzer (Mbsa.exe for the graphical user interface version; Mbsacli.exe for the command-line version). For more information about the Microsoft Baseline Security Analyzer, see article Q320454, “Microsoft Baseline Security Analyzer (MBSA) Version 1.0 Is Available,” 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>.

When you finish running auditing and diagnostic tools, restart the computer and log on under the local Administrator account.

#### 5. Perform final cleanup tasks.

Clear the Event Viewer log files and clear the Administrator account password. You can set the password in the Sysprep.inf file, or you can let end users choose a password; if a password is present when you run Sysprep, every computer will have the same Administrator password and you will not be able to change it during Mini-Setup. Finally, empty the Recycle Bin and clear the Start menu list, which includes command, program, document, and Internet Explorer history.

---

## Choosing Sysprep Settings

Sysprep prepares a master installation for disk imaging. You can run Sysprep at the command line or within the Windows graphical user interface. You need to put the Sysprep files in the Sysprep folder on each of your master installations or on a floppy disk.

### Running Sysprep

You run Sysprep just before you create a disk image of a master installation. This ensures that any changes Sysprep makes are present on the disk image, which in turn ensures that the changes are present on every destination computer onto which you copy the disk image.

When you run Sysprep without specifying any parameters, Sysprep:

- Searches for Sysprep.inf, and, if the file is found, temporarily stores the path to Sysprep.inf in the registry.
- Determines whether a master computer is a member of a domain, and, if it is, removes the master computer from the domain.
- Copies Setupcl.exe to *systemroot\System32*, and then runs Setupcl.exe, which resets SIDs.
- Removes all network adapters (except legacy network adapters), which removes all network settings such as DNS and IP configuration settings.
- Configures the registry so that Mini-Setup runs the next time a destination computer is started.
- Issues a shutdown command so a disk image of the master installation can be created.

You can run Sysprep on a master installation without specifying any parameters if:

- You do not want to perform any auditing or testing after a disk image is copied onto a destination computer and before it is delivered to an end user.
- You are not performing automated installation and configuration tasks by using a Winbom.ini file.
- You do not want to install or configure software, device drivers, or system components after a disk image is copied onto a destination computer and before it is delivered to an end user.
- You do not need to enumerate non-Plug and Play devices the first time a destination computer starts.
- Your master computer shuts down properly after you run Sysprep. Some computers do not shut down after you run Sysprep; if this is the case, you must use the **-forceshutdown** parameter with Sysprep.
- You do not want to reset the grace period for Windows Product Activation, nor clear the critical devices database, nor run Sysprep without generating new SIDs.

If you cannot run Sysprep with its default settings, you need to specify optional parameters. You can use the following guidelines to help you configure Sysprep.

#### Using the **-activated** parameter

Use the **-activated** parameter if you activate your destination computers in Factory mode. For more information about Windows Product Activation and Sysprep, see article Q299840, “How to Use Sysprep with Windows Product Activation or Volume License Media to Deploy Windows XP,” 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>. The **-activated** parameter is not applicable if you have a volume license.

#### Using the **-audit** parameter

Use the **-audit** parameter to audit or test a computer in Factory mode. If you use this parameter, you must clear the event logs and delete all files that you created while you were auditing or testing. You cannot use the **-audit** parameter with any other Sysprep parameters.

#### Using the **-bmsd** parameter

Use the **-bmsd** parameter to populate the [SysprepMassStorage] section of Sysprep.inf with the Plug and Play IDs of mass-storage devices specified in Machine.inf, Scsi.inf, Pnp SCSI.inf, and Mshdc.inf. Sysprep only builds the list of mass-storage devices; it does not install these devices in the critical device database or complete any other processing.

You can only use this parameter if the [SysprepMassStorage] section exists in Sysprep.inf, but does not contain any entries. You do not need to add the BuildMassStorageSection parameter to the [Sysprep] section in Sysprep.inf when you use the **-bmsd** parameter. In addition, you cannot use the **-bmsd** parameter with any other Sysprep parameters.

**Using the -clean parameter**

Use the **-clean** parameter to delete device drivers for mass storage controllers that are loaded but not physically present on a computer. You can only use the **-clean** parameter if you used the [SysprepMassStorage] section in Sysprep.inf and the **-bmsd** parameter to load device drivers for mass storage controllers. You typically run Sysprep with the **-clean** parameter in a Cmdlines.txt file. You cannot use the **-clean** parameter with any other Sysprep parameters.

**Using the -factory parameter**

Use the **-factory** parameter to perform installation and configuration tasks — such as installing, configuring, auditing, or testing software and system components — before you prepare a computer for delivery to an end user. You must run Sysprep again on the destination computer when you are finished performing installation and configuration tasks in Factory mode. To do this, use the Reseal and ResealMode entries in the [Factory] section of Winbom.ini.

**Using the -forceshutdown parameter**

Use the **-forceshutdown** parameter if a computer with an ACPI BIOS does not shut down after you run Sysprep.

**Using the -noreboot parameter**

Use the **-noreboot** parameter to test installation and configuration changes in a nonproduction environment. When you run Sysprep with this parameter, Sysprep performs all tasks without shutting down or restarting the computer.

**Using the -nosidgen parameter**

Use the **-nosidgen** parameter if you are not duplicating the computer on which you are running Sysprep.

**Using the -pnip parameter**

Use the **-pnip** parameter only if legacy (non-Plug and Play) hardware is not being detected properly. The **-pnip** parameter can only be used to install legacy hardware, such as COM ports, and cannot be used to install unsigned device drivers. In addition, a destination computer can take up to 20 minutes to start when you use the **-pnip** parameter. This is because the **-pnip** parameter forces a computer to enumerate every device.

**Using the -quiet parameter**

Use the **-quiet** parameter to run Sysprep without displaying onscreen confirmation messages. This is useful if you are automating Sysprep. For example, if you plan to run Sysprep immediately following an unattended Setup, add **sysprep -quiet** to the [GuiRunOnce] section of the Unattend.txt file.

**Using the -reboot parameter**

Use the **-reboot** parameter to force a computer to automatically reboot and then start Mini-Setup, or Factory mode, as specified. This is useful when you want to audit the system and verify that the first-run experience is operating correctly.

**Using the -reseal parameter**

Use the **-reseal** parameter to prepare a destination computer for final delivery to an end user after you have performed installation and configuration tasks in Factory mode. This parameter clears the Event Viewer logs and configures the registry so that Mini-Setup is set to start at the next boot. If you run the command **sysprep -factory**, you must seal the installation as the last step in your preinstallation process, either by running the command **sysprep -reseal** or by clicking the **Reseal** button in the **Sysprep** dialog box.

For more information about Sysprep parameters, see the *Microsoft Windows Corporate Deployment Tools User's Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.

---

## Creating Disk Images of Master Installations

After you run Sysprep on a master installation, you can create the disk image by using a third-party program. Microsoft does not provide a disk-imaging program.

Disk imaging typically involves the following steps:

1. Start the master computer by using a floppy disk, CD, or DVD. The third-party disk-imaging product includes a startup disk or CD that contains the imaging software.
2. Run the third-party disk-imaging program to create an image of the master installation.
3. Save the image in a shared folder, or write the image directly to a CD or DVD.
4. Shut down the master computer.

The disk-imaging process might vary depending on the disk-imaging software you use. Refer to the documentation that came with your disk-imaging software to design your disk-imaging process.

**Caution**

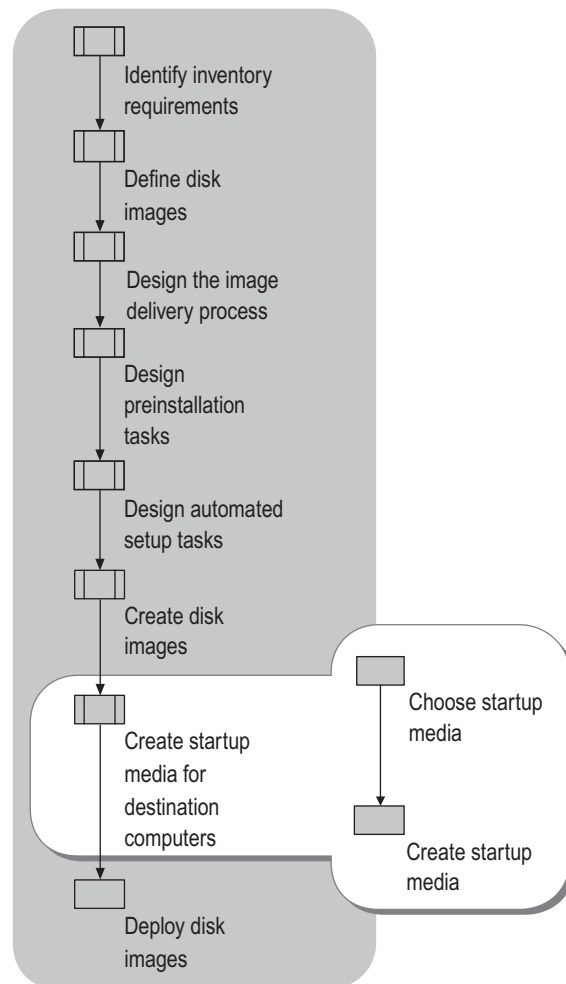
After you use Sysprep to prepare a master installation, you must not reset SIDs or perform other system preparation tasks by using third-party disk-imaging programs. Doing so after you run Sysprep can damage your master installation and make your disk image unusable. Furthermore, resetting SIDs by using a third-party tool is not supported.

# Creating Startup Media for Destination Computers

Before you can copy a disk image onto a destination computer, you need to start the destination computer from some type of startup media, such as a floppy disk, CD, or DVD. Some disk-imaging programs provide startup media; some do not. If your disk-imaging program provides startup media, use the media and the instructions that came with it to start your destination computers. If your disk-imaging program does not provide startup media, you need to create the startup media yourself.

Figure 3.8 shows the process you follow to create startup media.

**Figure 3.8 Creating Startup Media for Destination Computers**



## Choosing Startup Media

Choosing startup media is a multistep process. First, you determine what type of startup media your hardware supports. Not every computer can support CD or DVD startup media. Next, you determine whether one particular type of startup media is more appropriate than another, based on the way you are performing your image-based installations.

### Evaluating Hardware Support for Startup Media

Follow these steps to determine what type of startup media your organization can support.

1. Evaluate your hardware inventory for floppy disk support.

To use a floppy disk as startup media, every destination computer must have a floppy disk drive and the boot-order sequence in every BIOS must list the floppy disk drive.

2. Evaluate your CD or DVD writable device.

To use a CD or DVD as startup media, you must have the proper hardware, software, and instructions to create bootable CDs or DVDs. Microsoft does not provide any tools for creating CD or DVD startup media; however, several manufacturers provide the hardware, software, and system files that you need to create bootable CDs or DVDs.

3. Evaluate your hardware inventory for CD or DVD support.

To use a CD or DVD as startup media, all of your destination computers must have bootable CD-ROM or DVD drives. Some older CD-ROM drives and many DVD drives are not bootable devices. In addition, the boot-order sequence in the BIOS of each computer must include the CD-ROM or DVD drive. Some older BIOSes do not let you add the CD-ROM or DVD drive to the boot-order sequence.

If your organization supports only floppy disk startup media, you are ready to create your startup media. For more information about creating startup media, see “Creating Startup Media” later in this chapter.

### Identifying Which Startup Media to Use for Image-based Installation

If you have the proper hardware and software to create CD or DVD startup media, and the destination computers in your organization support CD or DVD startup media, you need to determine which type of startup media is best for your image-based installation. You can use the following guidelines to determine which type of startup media to choose.

Use a floppy disk to start your destination computers if:

- You are distributing disk images across a network.
- You do not need to create partitions or format disks before you copy the disk image onto the destination computer, or your disk configuration tools do not fit on a floppy disk.

Use a CD or DVD to start your destination computers if:

- You are distributing disk images on media (CD or DVD). You can put the disk image on the same media that you use to start the destination computer.
- You are configuring disk settings on destination computers before the disk image is copied onto the destination computer. You can put your disk configuration tools, scripts, and batch files on the same media that you use to start the destination computer.

---

## Creating Startup Media

Startup media contains the system files and device drivers that are necessary to start a computer so that the primary hard disk is accessible but not in use. Startup media might also contain network adapter and network drivers, CD and DVD device drivers, disk configuration tools, and scripts or batch files. The method you choose depends mostly on personal preference and your organization's capabilities; however, there are a few guidelines to follow:

- Your startup media must provide network support if you are distributing disk images across a network.
- Your startup media must provide CD or DVD device support if you are distributing disk images on media and you are using a floppy disk as your startup media.
- Your startup media must support the tools you need to copy a disk image from a storage location onto a destination computer. For example, if your startup media is an MS-DOS boot disk, you need to use MS-DOS tools to copy the disk image onto the destination computer.

You can use the following methods to create startup media.

**Create a TCP/IP boot disk** You can use an operating system CD for the Microsoft® Windows NT® Server version 4.0 operating system to create startup media if you are distributing disk images across a network. You must create a separate disk for each network adapter. For more information, see the TCP/IP Boot Disk link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

**Create a network boot disk by using Windows 2000** You can use the Network Client Administrator and a computer running the Windows 2000 operating system to create startup media if you are distributing disk images across a network. You must have a Windows NT Server 4.0 operating system CD. For more information, see article Q252448, “How to Create an MS-DOS Network Startup Disk in Windows 2000,” 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>.

**Create a network boot disk by adding NDIS drivers to an MS-DOS boot disk** You can use this method if you are distributing disk images across a network. You must create a separate disk for each network adapter. You must have an MS-DOS boot disk that was created by using the Network Client Administrator, which is included in the \Clients folder on the Windows NT Server 4.0 operating system CD. For more information, see articles Q142857, “How to Create a Network Installation Boot Disk,” and Q128800, “How to Provide Additional NDIS2 Drivers for Network Client 3.0,” in the Microsoft Knowledge Base. To find these articles, see the Microsoft Knowledge Base link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

**Create an MS-DOS boot disk** You can create an MS-DOS boot disk by right-clicking a floppy disk drive in Windows Explorer, clicking **Format** on the shortcut menu, and then selecting the **Create an MS-DOS startup disk** check box.

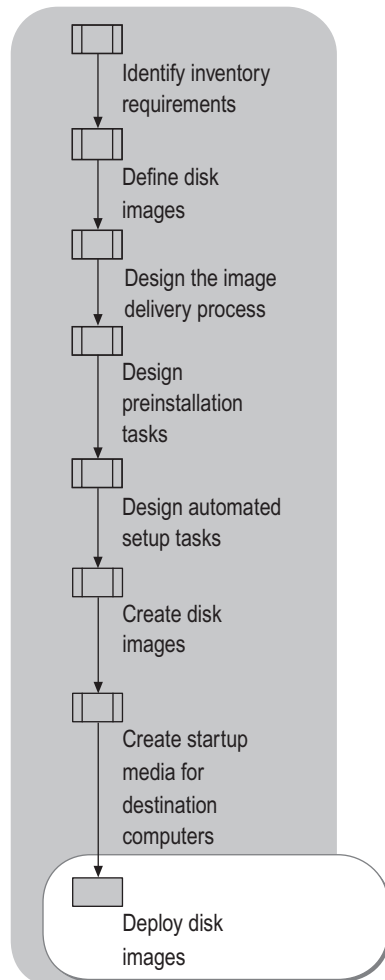
**Create a bootable CD or DVD** You can use your writable CD or DVD device to create bootable CDs or DVDs. You can also create a bootable CD according to the El Torito specification. For more information about using the El Torito specification to create a bootable CD, see article Q167685, “How to Create an El Torito Bootable CD-ROM,” 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>.



# Deploying Disk Images

The final step in your imaged-based installation, shown in Figure 3.9, is to deploy disk images. To deploy disk images, implement the procedures or tasks described in your user state migration plan (if you have one). Then, start the destination computer by using your startup media, and implement the procedures or tasks described in your disk configuration plan (if you have one). When you are finished implementing your disk configuration plan, use your disk-imaging program to copy the disk image to the destination computer, and then shut down the destination computer. Finally, if you are not using Factory mode to configure the destination computer, deliver the destination computer to the end user. If you are using Factory mode, start the computer, let Factory mode perform the configuration tasks specified in Winbom.ini, and then deliver the computer to the end user.

**Figure 3.9 Deploying Disk Images**



# Additional Resources

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

## Related Information

- “Choosing an Automated Installation Method” in this book for more information about planning Sysprep installations.
- “Designing Unattended Installations” in this book for more information about answer files, distribution shares, and unattended and automated installations.
- “Migrating User State” in this book for more information about migrating user data and settings.
- The *Server Management Guide* of the *Windows Server 2003 Resource Kit* (or see the *Server Management Guide* on the Web at <http://www.microsoft.com/reskit>) for more information about disk partitions and file systems.
- *Microsoft Windows Corporate Deployment Tools User's Guide* (Deploy.chm) for more information about using Sysprep. Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.
- The Windows Catalog link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources> for information about using the Windows Catalog.
- The Windows Update link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources> for information about Windows Update.
- The Windows Preinstallation Environment link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources> for information about Windows PE and Windows PE licensing plans.
- The Microsoft Platform SDK link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources> to download the Core SDK, which contains information about configuring a .theme file.
- The TCP/IP Boot Disk link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources> for more information about creating a TCP/IP boot disk for distributing disk images across a network.
- Article Q216573, “How Windows Determines ACPI Compatibility,” and article Q298898, “How to Determine the Hardware Abstraction Layer (HAL) That Is Used in Windows XP,” in the Microsoft Knowledge Base for more information about determining the type of HAL that is installed on a computer. To find these articles, see the Microsoft Knowledge Base link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

- Article Q294895, “Description of the Application Compatibility Toolkit 2.0 for Windows XP,” 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>.
- Article Q298389, “Sysdiff.exe Deployment Tool Is Not Included in Windows XP,” in the Microsoft Knowledge Base for more information about other resources that are similar to Sysdiff.exe. To find this article, see the Microsoft Knowledge Base link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.
- Article Q271369, “Statically-Entered TCP/IP Settings Are Not Present After Sysprep,” in the Microsoft Knowledge Base for more information about how Sysprep affects network settings. To find this article, see the Microsoft Knowledge Base link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.
- Article Q257813, “Using Sysprep May Result in ‘Stop 0x7B (Inaccessible Boot Device)’ on Some Computers,” in the Microsoft Knowledge Base for more information about Stop 0x7B errors. To find this article, see the Microsoft Knowledge Base link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.
- Article Q299840, “How to Use Sysprep with Windows Product Activation or Volume License Media to Deploy Windows XP,” in the Microsoft Knowledge Base for more information about Windows Product Activation and Sysprep. To find this article, see the Microsoft Knowledge Base link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.
- Article Q252448, “How to Create an MS-DOS Network Startup Disk in Windows 2000,” in the Microsoft Knowledge Base for more information about creating a network boot disk by using a Windows NT Server 4.0 operating system CD. To find this article, see the Microsoft Knowledge Base link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.
- Article Q167685, “How to Create an El Torito Bootable CD-ROM,” in the Microsoft Knowledge Base for more information about using the El Torito specification to create a bootable CD. To find this article, see the Microsoft Knowledge Base link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.
- Articles Q142857, “How to Create a Network Installation Boot Disk,” and Q128800, “How to Provide Additional NDIS2 Drivers for Network Client 3.0,” in the Microsoft Knowledge Base for more information about creating a network boot disk by adding NDIS and NDIS2 drivers to an MS-DOS boot disk. To find these articles, see the Microsoft Knowledge Base link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

**Related Tools**

- Sysprep.exe, Setupcl.exe, and Factory.exe

Use Sysprep.exe, Setupcl.exe, and Factory.exe to prepare a hard disk for disk imaging. To obtain Sysprep, open the Support\Tools folder on any Windows XP Professional or Windows Server 2003 operating system CD, and then open Deploy.cab. You can also see the Windows Downloads link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

- Windows Upgrade Advisor

Use Windows Upgrade Advisor to identify incompatible software and hardware on a destination computer before you perform an image-based installation. To download the Upgrade Advisor tools, see the Windows Upgrade Advisor link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>. You can also run the Windows Upgrade Advisor tools by using the **/checkupgradeonly** parameter with the Winnt32.exe tool. The Winnt32.exe tool is included in the I386 folder on the Windows XP Professional and Windows Server 2003 operating system CD.

- User State Migration Tool

Use the User State Migration tool to save user settings and data before you perform an image-based installation. To download a free version of the User State Migration tool, see the User State Migration Tool link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

- Microsoft Baseline Security Analyzer

Use the Microsoft Baseline Security Analyzer to identify security vulnerabilities that require further configuration after you perform an image-based installation. See article Q320454, “Microsoft Baseline Security Analyzer (MBSA) Version 1.0 Is Available,” 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>.

**Related Job Aids**

- “Disk Image Worksheet” (ACISYS\_1.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Disk Image Worksheet” on the Web at <http://www.microsoft.com/reskit>) for a worksheet to help you define your disk images.
- “Mass Storage Controller Worksheet” (ACISYS\_2.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Mass Storage Controller Worksheet” on the Web at <http://www.microsoft.com/reskit>) for a worksheet to help you record information about your mass storage controllers.

# Designing RIS Installations

4

Use Remote Installation Services (RIS) to simplify the installation of operating systems on client computers in your organization by performing remote image- and CD-based installations on client computers with no operating system or on failed computers that need restoration of the operating system. RIS enables you to create, maintain, and quickly install identical operating system and software configurations on multiple remote client computers with a predefined level of end-user interaction.

## In This Chapter

<b>Overview of the RIS Deployment Process .....</b>	<b>162</b>
<b>Planning RIS Installations.....</b>	<b>172</b>
<b>Designing RIS-based Installations.....</b>	<b>215</b>
<b>Configuring and Deploying RIS .....</b>	<b>278</b>
<b>Deploying an Operating System.....</b>	<b>290</b>
<b>Additional Resources.....</b>	<b>291</b>

## Related Information

- For information about Sysprep installations, see “Designing Image-based Installations with Sysprep” in this book.
- For information about unattended installations, see “Designing Unattended Installations” in this book.

# Overview of the RIS Deployment Process

RIS enables you to support on-demand image-based or script-based clean operating system installations over a network connection from a RIS server to a RIS client. RIS is included in Microsoft® Windows® Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; and Windows Server 2003, Datacenter Edition operating systems. RIS allows you to standardize client operating system installations, control the end-user installation experience, and choose the software distribution media you use. RIS supports large-scale deployments of Windows Server 2003 and Microsoft® Windows® XP Professional and can also serve as an operations and recovery tool.

RIS uses Pre-boot eXecution Environment (PXE) technology to enable client computers without an operating system to boot remotely to a RIS server that performs installation of a supported operating system over a TCP/IP network connection. You can deploy one or more RIS servers to accommodate your client operating system needs, but each client must have compatible hardware, which includes a BIOS and network adapter that support the remote-boot process. You can create different sets of RIS images to accommodate various configurations of different groups of client computers. You can also use Group Policy settings to limit the installation options that RIS presents to clients. You can use RIS to provide interactive operating system installations that require user input, or fully-automated installations that require no user input other than logon credentials.

The process steps described in this chapter can help IT professionals in medium and large organizations successfully plan, design, and execute a RIS-based operating system deployment. Job aids that are available to assist you in deploying RIS are listed in “Additional Resources” later in this chapter.

It is recommended that you use RIS when you have a large number of clients that need clean installations of an operating system and when you have an idea of the software configurations you want to deploy in your organization. To deploy RIS, your network infrastructure must be able to support RIS-based installations. Also, DNS and Dynamic Host Configuration Protocol (DHCP) servers must be running on the network and you must have the Active Directory® directory service installed. In addition, you must be familiar with the Windows XP Professional and Windows Server 2003 setup process.

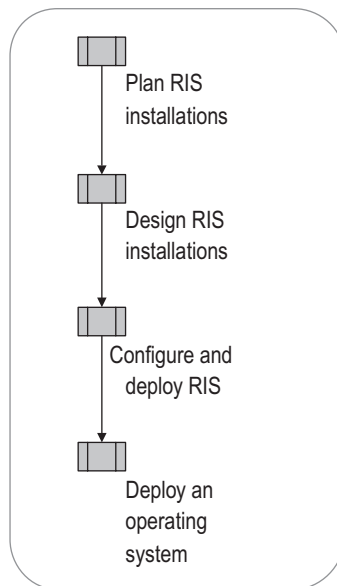
Once you deploy RIS, you can automate large-scale operating system installations, customized for various predefined client and server configurations, in either the interactive or fully-automated mode. You can deliver standard desktops to clients using predefined master images, including customized application installation and configuration. You can also provide installations based on CD-type images from a distribution share. In addition, you can secure client installations by setting user access rights and configuring Group Policy settings that control user installation options.

## Process for Deploying RIS

The RIS deployment process consists of three phases including planning, design, and configuration and deployment. You will need a design team to handle the planning and design phases and a deployment team for the configuration and deployment phase.

Figure 4.1 illustrates the process steps for deploying RIS in your organization, followed by the deployment of an operating system.

**Figure 4.1 Deploying RIS**



## **RIS Deployment Teams**

Design team personnel might consist of high-level system architects who make planning decisions and designers who are upper-tier administrators that choose the appropriate methods for carrying out the planning decisions. Deployment team personnel might consist of lower-tier administrators and technicians who implement the design decisions.

Some of the responsibilities of the design team include tasks such as evaluating the current environment, assessing RIS network security, and evaluating image requirements, in addition to designing the overall installation configuration, the supporting infrastructures, the RIS server configuration, and a RIS test environment.

Some of the responsibilities of the deployment team include tasks such as configuring the network infrastructure to support RIS, creating and configuring RIS servers, creating images, customizing answer files, creating client boot disks, and designing the Client Installation Wizard (CIW) process. The deployment team also deploys the operating systems.

## **RIS Technology Background**

RIS was introduced in Microsoft® Windows® 2000 to allow server-based installation of an operating system onto client computers that do not currently contain one. Improvements to RIS in the Windows Server 2003 family are summarized in the following section.

### **New in Windows Server 2003**

With the release of Windows Server 2003, RIS now supports the following new capabilities:

- Deployment of Microsoft® Windows® 2000 Professional, Microsoft® Windows® 2000 Server, Microsoft® Windows® 2000 Advanced Server, Windows XP Professional, and the Windows Server 2003 family operating systems.
- Automation of the CIW using the Autoenter feature.
- Enhanced cross-domain functionality.
- Increased security by adding a masked double-prompt administrator password.
- Automatic DHCP authorization with Risetup.exe.
- Auto-detection of the target system Hardware Abstraction Layer (HAL) type to allow filtering of images from the CIW.



- Support for the Recovery Console and support for Microsoft® Windows® Preinstallation Environment.
- Support for Microsoft® Windows® XP 64-Bit Edition Version 2003 and the 64-bit versions of the Windows Server 2003 family.
- Support for the Uniqueness Database in .sif files.
- Support for Secure Domain Join.
- Support for NTLM version 2 (NTLMv2)
- Support for encrypted local administrator password entries.

## RIS Components

RIS consists of several components that facilitate the remote installation of client operating systems. To create the RIS server configuration, you must install the **Remote Installation Services** Windows component from **Add or Remove Programs** in **Control Panel**. This component configures and starts the following services:

**Remote Installation Services (Binlsvc)** This service detects PXE-initiated DHCP requests from RIS clients and facilitates a response to those requests. Remote Installation also directs clients to files on the RIS server that initiate the installation process and then services CIW requests. In addition, Remote Installation checks Active Directory to verify client credentials, determines if a client can be serviced, and confirms whether to create a new computer account object or reset an existing account on behalf of the client. Also, if a client that is prestaged in Active Directory has settings specifying that a particular RIS server must answer the client, then Remote Installation facilitates the response to that client from the specified RIS server.



### Note

The Remote Installation Service was formerly known as the Boot Information Negotiation Layer (BINL) service in Microsoft® Windows® 2000 and Windows XP Professional.

**Trivial File Transfer Protocol Daemon (TFTP)** A RIS server uses TFTP to download the CIW and the initial files needed to start the remote installation process on the client computer.

**Note**

On a RIS server, TFTP is called a *daemon* or service (TFTPD) while on the client side it is referred to as a *protocol* (TFTP).

The first file that downloads is Startrom.com, which is a small bootstrap program that displays the **Press F12 for Network Boot** prompt to the client. If the user presses F12 within 3 seconds, the CIW downloads to the client so the installation process can begin. The file Startrom.com is located on your RIS server in the directory path `\\ServerName\RemoteInstall\OSChooser\i386\`.

**Note**

For installations of Windows XP 64-Bit Edition Version 2003, the first file downloaded is Oschoice.efi. It is not necessary to press F12 for these installations.

**Single Instance Store (SIS) Service** SIS consists of an NTFS file system filter driver and a groveler agent that interacts with RIS images. The SIS service reduces the hard disk storage requirements for RIS images. SIS does this by monitoring the RIS server partition for duplicate files. Whenever the groveler agent finds a duplicate file, SIS copies the original file into a directory and an NTFS reparse point containing the current location, size, and attributes of the original file. This way, SIS retains only a single instance of the file while replacing duplicate files with links to the single instance. This enables SIS to store the duplicate files it finds in RIS images and reduce disk space usage on your RIS server.

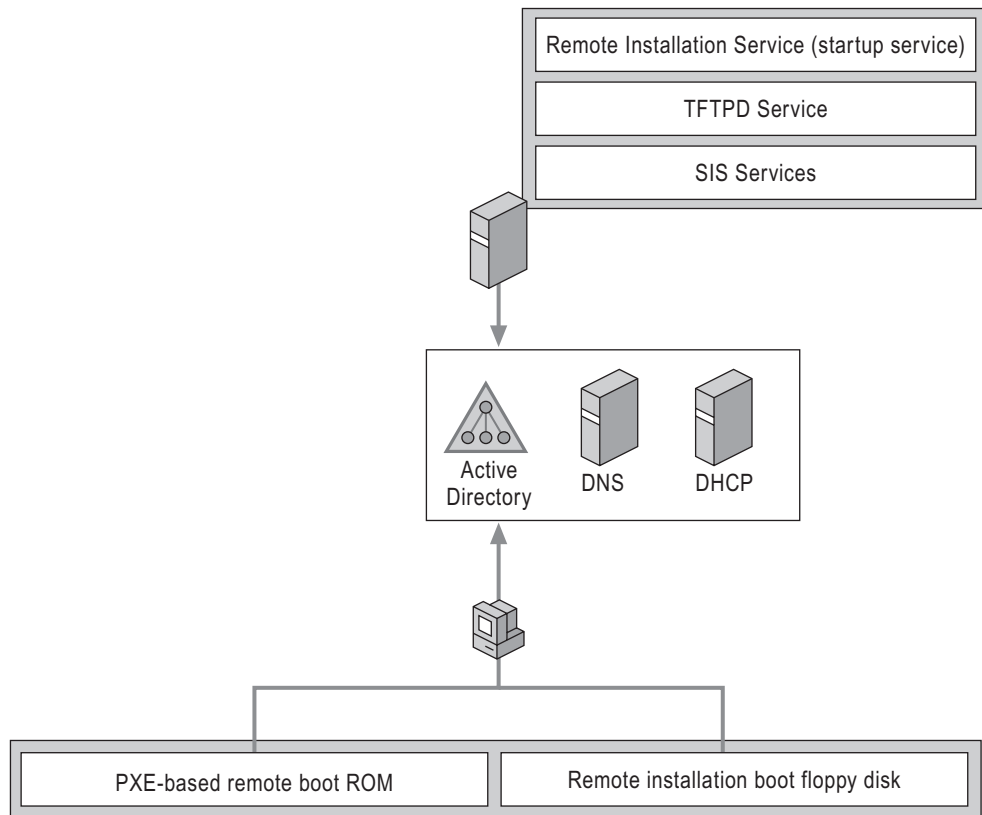
**Caution**

When backing up a RIS server, you must use an SIS-aware backup solution. Failure to use an SIS-aware backup solution while backing up a RIS server consumes unnecessary disk space while performing a restore operation and might result in some of your files not being restored. The backup program included in Windows Server 2003 is SIS-aware.

## Remote Boot and Installation Setup Processes

RIS uses PXE technology to allow RIS clients without an operating system to initiate the boot sequence from their network adapters, thus facilitating operating system installations from remote network locations. To initiate the remote boot process and set up a RIS-based operating system installation, PXE interacts with the Dynamic Host Configuration Protocol (DHCP), the Remote Installation services, and the TFTP, as shown in Figure 4.2.

**Figure 4.2 RIS Installation Configuration**



When you start a new PXE-enabled RIS client computer, the following sequence of events occurs:

1. The client computer initiates the communication by sending a DHCP Discover broadcast on its subnet. A DHCP server with an active scope for that subnet will issue an IP address to the client.
2. All Remote Installation servers that receive the client's DHCP Discover broadcast extract (from the PXE data portion of the packet) the UUID of the client that is requesting service. The RIS server then queries its preferred domain controller to search for this UUID in all prestaged computer accounts in Active Directory.

If the domain controller does not find the UUID in the local domain, the RIS server queries the global catalog to locate the client computer account. If the UUID is found in either location, the client computer is recognized as a known client; otherwise, it is an unknown client. If the client is unknown, it will only receive an answer from a RIS server that is configured to answer unknown clients, provided one exists on the network.

3. If the client is known, all available RIS servers query the domain to determine whether the prestaged client computer account has a setting that specifies that only a particular RIS server can answer the client.

If this is the case, then only the designated RIS server answers the service request, and other RIS servers simply notify the client of the particular RIS server configured to answer it. If the client computer account does not have a setting that requires it to be answered by a particular server, any RIS server can answer the request. However, the client only receives service from the first RIS server it contacts.

4. The user receives a prompt to press the F12 key to initiate a network service boot request from the RIS server.
5. Using the TFTP daemon (service), the contacted RIS server downloads the CIW to the RIS client, along with all client dialog boxes contained within the CIW.
6. The CIW prompts the user to log on with a valid user name, password, and domain name.
7. The user receives an offering of operating system images hosted on the RIS server for installation on the client computer.

The list of operating system images offered to the user is based on the user's credentials or security group membership.

## PXE Specifications

The published PXE specification defines the remote boot process and also establishes the PXE compliance standards for hardware manufacturers and other vendors. RIS uses PXE environment extensions to DHCP, an industry-supported technology, to allow workstations to do the following:

- Boot remotely using their network adapters to access bootstrap code from a network location.
- Install an operating system from a remote source to a client's local hard disk.

The PXE environment is built upon Internet protocols and services that are widely used in the computer industry. This includes TCP/IP, DHCP, and TFTP. The PXE extensions to the DHCP protocol enable information to be sent to network-bootable systems and also allow these systems to locate remote installation services. For more information about PXE and the protocols required to support network booting, see the Preboot Execution Environment (PXE) Specification link on the Web Resources page at: <http://www.microsoft.com/windows/reskits/webresources>.



### Note

Network adapters that meet the PXE .99n specification should work correctly with RIS.

## RIS Components

The following RIS components enable you to install, configure, and implement RIS in your organization.

**Remote Installation Services** An optional Windows component that you can install with Windows Server 2003 or you can add it at any time after the operating system installation. Services that install with RIS include Remote Installation, TFTP, and the SIS Groveler.

**Remote Installation Services Setup (Risetup.exe)** You use this component to initially set up the RIS server and create at least one CD-based operating system image. You can initiate the setup process from the **Start** menu of your RIS server. By selecting **Remote Installation Services Setup** from the **Administrative Tools** group, a wizard starts and does the following:

- Requests preliminary information, including the installation folder name and the path to the operating system installation files.
- Copies Windows installation files.
- Updates the CIW screens.

- Creates a default answer file (Ristndrd.sif).
- Starts RIS services.
- Authorizes the DHCP server.

**Note**

Rissetup is also used to create any additional CD-based operating system images after the initial installation is created.

**Remote Installation Preparation Wizard (Riprep.exe)** Riprep.exe allows you to create a customized image of an operating system such as Windows XP Professional. To create an image means that you create a replica of a hard disk that you can install on other computers in your organization. You use Riprep to image an existing Windows XP Professional operating system installation on a master computer and replicate that image to an available RIS server on your network. The image can include the operating system with default parameters applied, or the operating system with a preconfigured desktop, locally-installed applications, and drivers.

**Remote Boot Floppy Generator (Rbfg.exe)** Rbfg.exe allows you to create remote boot floppy disks for some RIS clients that are not PXE-enabled, so that these clients can emulate the remote boot process and install an operating system over the network using RIS. However, for non PXE-enabled RIS clients to use the remote boot floppy disk, they must each have a supported Peripheral Component Interconnect (PCI) network adapter.

**Client Installation Wizard (OSChooser)** The OSChooser is the client-side service of the CIW. It is a text-based program downloaded by the RIS server that allows the client to communicate with the RIS server during setup of the installation process. Remote Installation is the server-side component that sends a default set of CIW screens to guide the client through the remote installation process. Remote boot-enabled clients use the CIW to log on and select from operating system installation options. You can customize these setup screens to meet the needs of your organization.

**Active Directory Users and Computers Extension for RIS (Dsa.msc)** When you create the RIS server, the Active Directory Users and Computers extension installs on the RIS server. The extension provides a **Remote Install** tab within the computer account **Properties** dialog box of each RIS server that allows you to administer the RIS server. You can start this extension by specifying the Microsoft Management Console (MMC) snap-in Dsa.msc in the **Run** dialog box or you can start it from the command line.

You can administer RIS locally or through a Terminal Services session on another network computer. You can also administer RIS from a computer running Windows XP Professional if you install the Adminpak.msi on that computer.

## RIS Tasks

Table 4.1 describes some of the tasks that you might perform while using RIS, the corresponding RIS components you would use, and which users can perform the tasks.

**Table 4.1 RIS Components, Tasks, and Users**

Task	RIS Component	User
Install RIS	Remote Installation Services Windows component	Server administrator
Complete RIS server installation	Remote Installation Services Setup (Risetup.exe)	Server administrator
Configure Group Policy settings related to RIS	Active Directory Users and Computers RIS Extension (Dsa .msc)	Server administrator
Create operating system images, including application and desktop configurations, and install on RIS servers	Remote Installation Preparation Wizard (Riprep.exe)	Desktop administrator
Create boot floppy disk for non PXE-enabled client computers to install operating systems using RIS	Remote boot floppy generator (Rbfg.exe)	Desktop administrator
Provide log on and selection of operating system images to RIS clients	Client Installation Wizard (OSChooser.exe)	End user

## RIS Technology Limitations

You can use RIS technology to install operating systems, with or without software applications, to portable and desktop computers in your organization, which include member servers, stand-alone servers, and domain controllers. However, limitations to the scope of RIS-based operating system installations include the following:

**Clean Installs** You can only use RIS to provide a clean version of an operating system, with or without software applications. You cannot use RIS to upgrade an operating system or software configuration.

**Server Components** If you use RIS to install a server operating system, you might not be able to include all the server components you want to provide with the RIS image. For example, some server components require that you install and configure them only after the RIS-based installation is complete. This can include components such as Certificate Services, Cluster service, or software that is dependent on Active Directory.

**Domain controllers** You cannot install a preconfigured domain controller using a RIS image. However, you can use RIS to install a stand-alone server and then configure the server as a domain controller by running the Active Directory Installation Wizard.

**Encryption and security settings** You cannot use RIS to deploy files that are encrypted with a system such as the Encrypting File System (EFS). Also, you cannot use RIS to deploy systems with preconfigured user-level security settings such as file and folder permissions. To configure these settings, you can run a script after completing your RIS-based installation.

**Wireless networks** Wireless networks do not support pre-booting computers using PXE technology.

**Multihomed computers** Multihomed RIS servers are supported if the network adapters service multiple separate subnets or if all network adapters service the same subnet. In both cases the RIS server must also be the DHCP server. The DHCP server must have active scopes for each subnet serviced and must be authorized for each IP address on the network adapters being serviced.

**Supported operating systems** RIS has certain limitations depending on the operating system that you are installing. For more information about operating systems supported by RIS, see “Operating Systems supported by Remote Installation Services” in Help and Support Center for Windows Server 2003.

---

## Planning RIS Installations

Careful planning is critical to ensure successful RIS-based installations. Effective planning minimizes the time and effort required to support large-scale operating system installations across your organization.

In large organizations that support hundreds or even thousands of desktop computers, it is expensive and inefficient to manually install every operating system and respond to each dialog box that Setup displays. In this type of environment, the best approach is to use RIS to automate and customize the operating system installation process for your clients. An appropriate plan for custom RIS-based operating system installations lets you:

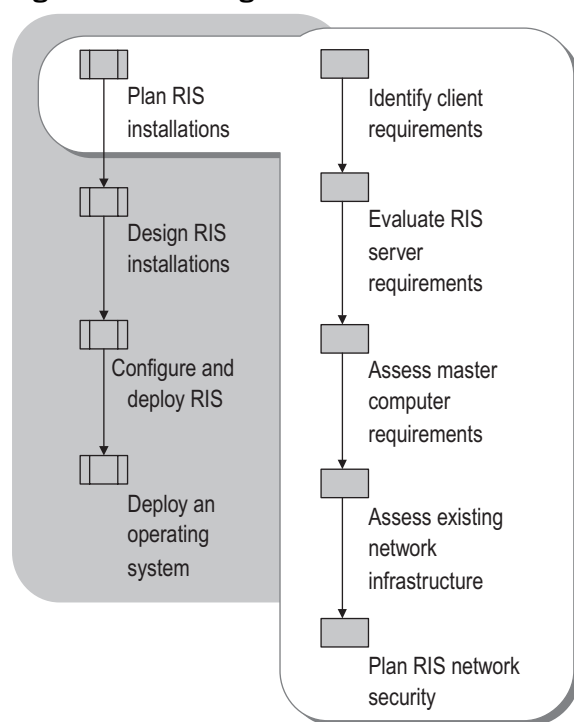
- Accommodate differing software and hardware configurations and varying user needs.
- Control the interaction level of end users during installations.
- Minimize the number of operating system images you need to manage.



Typically you would use a volume license for bulk rollouts of Windows XP or Windows Server 2003. If you would like to use individual product keys for each installation, you need to use the Windows Management Instrumentation (WMI) Windows Product Activation (WPA) provider. For more information about the WMI WPA provider, 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>.

When planning your RIS-based operating system installation, you must first gather the data you need to choose the appropriate configurations for your RIS servers and clients. The steps in this process are illustrated in Figure 4.3.

**Figure 4.3 Planning RIS Installations**



For additional information about Best Practices to assist your planning process, click the Index button in Help and Support for Windows Server 2003 and in the keyword box type **Remote Installation Services**, then select **Best Practices**.

## Identifying Client Requirements

If you have existing client computers on your network that you are considering for RIS-based operating system installations, you need to evaluate the hardware and software configurations of these clients during the planning phase. If you need to obtain new client computers to receive RIS-based operating system installations, you can acquire them from an OEM/Solution provider. For both new and existing clients, you need to determine if your clients satisfy the requirements for RIS-based installations.



### Important

You can only use RIS to perform clean operating system installations. You cannot use RIS to perform an operating system upgrade.

To identify requirements for RIS client computers on which you want to install an operating system by using a RIS-based installation, you need to:

- Evaluate whether your client computers meet the minimum hardware requirements for the operating system you intend to install.
- Determine if your client computers utilize the same HAL as the master computer (for Riprep images only).
- Evaluate the remote boot capabilities of RIS clients (whether they are PXE-enabled or if they require a RIS boot floppy disk).
- Audit existing client computers so you can inventory software and hardware configurations.
- Decide if you want to prestage RIS clients in Active Directory for more secure RIS-based operating system installations.
- Evaluate operating system configurations.

You can perform these tasks in any order. For more information about each task, see the sections that follow.

---

## Evaluating RIS Client Hardware

In general, RIS client computers must meet the requirements for the operating system that you install on them. Whether you are deploying a client or server operating system, it is still considered a client installation with respect to RIS. However, hardware requirements differ between computers that host client operating system software and those that host server operating system software.

For more information about Remote Installation Services system requirements, see “Remote Installation Services system requirements” in Help and Support Center for Windows Server 2003.

To verify whether your existing client hardware is compatible with Windows XP, see the Windows Catalog link on the Web Resources page at:  
<http://www.microsoft.com/windows/reskits/webresources>.

You can also verify hardware compatibility by consulting the following:

- **Hardware Compatibility List.** A list of software and hardware products that are compatible with Windows 2000 and earlier Windows operating systems. See the Hardware Compatibility List link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.
- **Windows XP Professional Upgrade Center.** A Microsoft website that provides information for verifying whether your system hardware and software is compatible with Windows XP Professional. See the Windows XP Professional Upgrade Center link on the Web Resources page at: <http://www.microsoft.com/windows/reskits/webresources>.

For more information about verifying software and hardware compatibility see “Designing Image-Based Installations with Sysprep” in this book.

For this part of your planning process, use job aid “Planning for RIS Clients” (ACIRIS\_01.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning for RIS Clients” on the Web at <http://www.microsoft.com/reskit>) to indicate whether client computers require hardware upgrades. Also indicate the domains or organizational units in which clients must receive an upgrade and the personnel you want to assign to the task.

---

## Determining RIS Client HAL Types

If you want to create an image-based RIS installation using the tool Riprep.exe, you first need to determine if your RIS clients have a HAL that is compatible with the master computer from which you create your image. For example, if the master computer where you run Riprep.exe has an Advanced Configuration and Power Interface (ACPI) HAL, then the client computers you designate to receive operating system images generated from that master computer must also have an ACPI HAL. The HAL type is indicated by the original file name of the file Hal.dll.

You need to ascertain how many different HAL types exist in your organization. This determines how many different master installations you will need with HALs that are compatible with the client HALs in your organization. To verify the HAL type on your client computers, you can do one of the following:

- Use a management tool such as Microsoft® Systems Management Server (SMS) to obtain your client inventory, from which you can determine the HAL types.
- View the properties of Hal.dll to determine the HAL types.

To view the properties of Hal.dll on a client computer:

► **To obtain the HAL type on a client computer**

1. In **Windows Explorer**, open the *systemroot*\System32 folder.
2. Right-click Hal.dll, and then click **Properties** on the shortcut menu.
3. In the **Item name** list on the **Version** tab, click **Original File name**.

The original file name that displays in the **Value** list (such as Halacpi.dll or Hal.dll) indicates the HAL type.

For more information about HAL, see “Designing Image-based Installations with Sysprep” in this book, to determine the type of HAL that is installed on the computer.

You can install RIS-based operating system images if any of the following conditions are true regarding HALs:

- The master and destination computer HALs are identical.
- The master and destination computers both have either uniprocessor or multiprocessor Advanced Programmable Interrupt Controller (APIC) HALs.
- The master and destination computers both have either uniprocessor or multiprocessor Advanced Configuration and Power Interface (ACPI) HALs.

For a listing of the HAL types that Windows XP Professional and Windows Server 2003 support, along with additional information about determining HAL types and identifying hardware that impacts image-based installations, see “Designing Image-based Installations with Sysprep” in this book.



**Tip**

By default the HAL auto-detect feature of Riprep.exe causes the CIW to filter images based on the HALs of the client computers. CIW only lists images with compatible HAL types. You must generate the operating system images from master computers that have HALs compatible with those of the RIS clients.

For this part of your planning process, use job aid “Planning for RIS Clients” (ACIRIS\_01.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning for RIS Clients” on the Web at <http://www.microsoft.com/reskit>) to indicate the number of different HAL types in your organization and whether you require multiple master installations to match the differing HAL types of client computers. Also specify the domains or organizational units where the clients exist.

## Evaluating Remote Boot Capabilities of RIS Clients

To initiate a RIS-based operating system installation, a RIS client must first perform a remote (network) boot by connecting to a RIS server over the network. When the RIS client locates and downloads the boot files located on the RIS server, CIW displays on the client and prompts the client to logon and begin the installation process. The best way to facilitate the remote boot is to use a PXE-enabled RIS client, which means that both the network adapter and BIOS of the RIS client support PXE.

However, if a RIS client does not have a PXE-enabled network adapter and a supporting BIOS, you can emulate PXE support by using a PCI-based network adapter that boots from a RIS boot floppy disk. The RIS boot floppy disk is a startup disk that simulates the PXE startup process for computers that lack a remote boot-enabled BIOS. To be able to use a RIS boot floppy disk, RIS client computers must meet the minimum processor, Random Access Memory (RAM), and hard drive specifications referenced in “Evaluating RIS Client Hardware” earlier in this chapter. By using the RIS boot floppy disk to emulate PXE support, you can enable RIS-based operating system installations on non-PXE-compliant client systems. The Remote Boot Floppy Generator (RBFG) utility allows you to generate RIS boot floppy disks for use with RIS clients that are not PXE-enabled.



### Note

The remote boot floppy generator does not support Windows XP 64-Bit Edition Version 2003 or the 64-bit versions of the Windows Server 2003 family.

## Verifying the RIS Client Remote Boot Configuration

You need to verify whether your RIS clients are PXE-enabled. To do this, you can check the documentation and historical records that came with the system. If you do not have this information, you need to do the following:

- Verify your RIS clients have PCI, Mini-PCI, or CardBus type network adapters. RIS clients can only perform a remote boot from these types of network adapters.
- Verify that the BIOS of your RIS clients is capable of using the network adapter as the primary boot device. A ROM BIOS that is at least version .99n satisfies this requirement.



### Note

Most computers that conform to the Net PC or PC98 specifications have a PXE remote boot-enabled network adapter and remote boot-enabled BIOS.

You might be able to obtain this information using a management system such as SMS or directly from inspection of the client computers.

However, it might be easier for you to use a remote script to determine whether the BIOS of client computers in a specified domain supports PXE-enabled remote booting. To do this, you can use the BIOS Information script, which you can find from the Remote Installation Scripts link on the Web Resources page <http://www.microsoft.com/windows/reskits/webresources>.). To return the BIOS information, run this script at the command line and specify the Active Directory domain name and the **getallbios** command. The returned information verifies if the BIOS of client computers supports PCI adapters and selectable booting. If so, then the BIOS supports remote booting from a network adapter.

**Note**

The BIOS information returned by the BIOS information script does not conclusively determine if your system is completely PXE-enabled. However, if the information indicates that the BIOS does not support PCI network adapters or does not have a selectable boot capability, then it is a certainty that the BIOS does not support PXE-enabled remote booting.

The BIOS information script uses Active Directory Service Interfaces (ADSI) to query the Active Directory “Computers” container to obtain the computer objects for which the BIOS information is returned. The script also uses Windows Management Instrumentation (WMI) technology to query each computer and return the specific BIOS information to the command line. You can also redirect this output to a text file that you specify. For the script to function properly, you must have WMI installed on both the computer running the script and the computers that you query with the script. In addition, you must have ADSI installed on the computer running the script.

Network adapter manufacturers can embed the PXE-based remote boot code on a chip as part of the network adapter. Some manufacturers create a version of PXE ROM code as part of the client system BIOS to support the PXE environment specification.

For RIS clients that are not PXE-enabled, you need to determine if they can use a RIS boot floppy disk. To use a RIS boot floppy disk, these clients must have a PCI-type network adapter because RIS boot floppy disks do not support Personal Computer Memory Card International Association (PCMCIA), CardBus, ISA, USB, or other non-PCI network adapters. You can generate the RIS boot floppy disks for these clients by running the Rbfg.exe utility. This utility is located on the RIS server in the following directory location:

`\\RISServerName\RemoteInstall\Admin\i386\Rbfg.exe`

**Note**

To view a list of supported PCI network adapters supported by Remote Boot Floppy Generator, run Rbfg.exe and click the Adapter List button on the displayed dialog box.

The RIS boot floppy disk also enables you to use RIS to install operating systems on portable computers. However, portable computers often use PCMCIA network adapters that PXE does not support, so you cannot use these adapters with RIS-based operating system installations. Alternatively, you can place the portable computer in a docking station that contains a PCI network adapter and use a RIS boot floppy disk to facilitate the installation. You cannot add network adapters to the RIS boot floppy disk you create with Rbfg.exe.

**Note**

You should not use the same docking station to install RIS for multiple portable computers.

For RIS clients that require the use of a RIS boot floppy disk, the boot sequence in the BIOS must be set so that booting the floppy disk occurs first. For PXE-enabled RIS clients, the BIOS must be set to allow booting from the network adapter.

**Important**

You can use these BIOS settings when you implement interactive installations. However, if you intend to use automated installations, you must ensure that the BIOS boot configuration is set to use the hard disk as the first boot device. For more information about automated installations, see “Fully-Automated Installation Design Background” later in this chapter.

For more information about the PXE environment, including its security context, see “PXE Specifications” earlier in this chapter.

For this part of your planning process, use job aid “Planning for RIS Clients” (ACIRIS\_01.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning for RIS Clients” on the Web at <http://www.microsoft.com/reskit>) to record whether client computers require:

- Upgrades to support PXE.
- The use of RIS boot floppies.
- BIOS upgrades to support selectable booting.

Also specify the domains where the clients exist and the personnel you want to assign to the upgrade tasks.

## Auditing Existing Clients

If you control your existing client computers using Systems Management Server or a similar management product, you can wipe these computers clean in preparation for a new RIS-based installation. However, before you do this, it is advisable to audit these client computers by:

- Conducting an inventory.
- Backing up all user data and settings.
- Obtaining client UUIDs.

In this part of your planning process, use job aid “Planning for RIS Clients” (ACIRIS\_01.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning for RIS Clients” on the Web at <http://www.microsoft.com/reskit>) to indicate your decisions to conduct an inventory, backup user data, and obtain client computer UUIDs. You can also specify the domains or organizational units to audit and the personnel you want to assign to inventory and backup tasks.

### Conducting an Inventory

You conduct an inventory to determine such things as the number of existing clients, the types of existing desktop configurations in your organization, hardware configurations, software and hardware compatibility, and existing applications. For more information about creating hardware and software inventories, see “Planning for Deployment” in *Planning, Testing, and Piloting Deployment Projects* of this kit.

#### Inventory-related factors that impact RIS installation planning

The following are some issues that can arise when conducting an inventory and how they can affect the RIS installation planning process. Your primary concern is how these issues affect the number of images you need to create.

**Number of existing clients** The number of clients that have differing requirements can give you an indication of the number of RIS images you might need to create. Also, the number of clients you have determines the tool you need to use for automating the installation process. If you have a large number of clients, RIS is a good choice for the task. If you have a small number of clients, you might be better off using the Winnt.exe or Winnt32.exe programs in unattended mode. For more information about unattended installations, see “Designing Unattended Installations” in this book.



**Existing desktop configurations** The types of existing desktop configurations in your organization provide an indication of the number of different RIS images and answer files you might need to create. Alternatively, you can apply a standard desktop to all clients in your organization, which reduces the number of RIS images and answer files you need to maintain.

**Hardware configuration types** The types of existing client hardware configurations you have affects the tool you use to create installation images, the hardware device drivers you add to a distribution image, and how you configure answer files.

For example, if you want to use Riprep to create file-system-based images of an operating system, the master computer and all destination client computers must have identical HAL types.

Also, if you have hardware not supported by the Mini-Setup process, which occurs after image installation, this affects how you create RIS-based installations. For example, if you have a SCSI hard disk device that is not supported during the text mode phase of Mini-Setup, you need to add the driver files for the SCSI device — along with its Textsetup.oem file — to the distribution folder that you create using Risetup. You must also modify the [MassStorageDrivers] section of the RIS default answer file to add values for the appropriate driver entries.

For more information about Mini-Setup, see “Riprep Image Design Background” later in this chapter.

**Software and hardware compatibility** You need to ensure that your existing client computers meet the software and hardware requirements that support installation of the operating system images you plan to make available to them.

For information about hardware compatibility, see the Windows Catalog link on the Web Resources page at: <http://www.microsoft.com/windows/reskits/webresources>

To verify software compatibility for your existing clients, you can use the **Application Compatibility Toolkit**, which contains documents and tools to help you diagnose and resolve application compatibility issues. For more information about verifying software and hardware compatibility, see “Designing Image-Based Installations with Sysprep” in this book.

**Application configurations** The application configurations that exist on client computers indicate what you need to include in the Riprep images you create or what you need to provide on the distribution folder you create using Risetup.

**Special hardware components**

As part of planning your RIS-based installation, you must inventory special peripherals, hardware devices, and software configurations because these components can affect the number of images you need to create. A special component might be an existing hardware device that Mini-Setup (which follows image installation) does not support. If you do not take these components into account in the planning phase, the RIS-based installation that you implement might fail.

Some of the special hardware components you might need to add to your inventory include:

- Mass storage controllers
- Portable computer devices
- Vendor-specific devices
- Legacy devices

**Note**

Most Plug and Play peripheral devices, such as sound cards, network adapters, modems, and video cards, have no impact on RIS-based installations. It is therefore unnecessary to inventory these devices because Setup automatically detects, installs, and configures them after the RIS image is copied to the destination computer.

For more information about inventories for special hardware and software components, see “Designing Image-Based Installations with Sysprep” in this book.

**Special software components**

The installation requirements of some applications might cause you to alter the way you perform a RIS-based installation or they might call for you to create separate images. For example, some applications require that you install them after the RIS installation is complete, rather than installing and configuring them in a master installation (for a Riprep image). Also, you might be able to install some applications only on portable computers but not on desktops. In this situation, you probably need to create separate RIS images.

Some of the special software components you might need to inventory include:

**Core software applications** These applications might include office productivity suites and anti-virus software. You typically install and configure core applications in your master installation, although you can add applications to a distribution share that you create with Risetup images. If you have any computers on which you do not want to install core applications or any computers that require special configuration settings for these applications, note these in your software inventory. You probably need to create separate images to accommodate these differences.

**Line-of-business applications** These applications might include accounting, database, or investment modeling programs. You need to identify the groups in your organization that require line-of-business applications because you might want to create separate RIS images for specific groups, especially if they require substantial configuration or take a long time to install.

**Applications with Active Directory dependencies** You need to identify any applications that depend on Active Directory. You cannot include these types of applications in a RIS image because you can only install and configure them after installation of a RIS image is complete.

**Third-party utilities and tools** These applications might include the diagnostic tools of a computer manufacturer or a suite of hardware-specific utilities for a portable computer that allow you to configure power options and other features. You might need to install these utilities and tools after installation of a RIS image is complete. You might also want to create a separate RIS image for the computers that require these utilities and tools.

**Service packs, hotfixes, and patches** Identify all service packs, hotfixes, and patches that are installed in your organization. Be sure you record the revision number and the revision date of the service pack, hotfix, or patch in your inventory.

## Migrating User State

You will need to create a user state migration plan if any of your destination computers contain any of the following items that you want to restore after installation is complete:

- User data that you want to be available to the end user. User data includes such things as documents, e-mail messages, spreadsheets, and databases.
- User settings such as desktop settings, shortcuts, and Microsoft® Internet Explorer Favorites.
- Application settings such as application-specific keyboard shortcuts, spell-checking options, and default file locations.

At a minimum, your user state migration plan must do the following:

- Identify the data you want to migrate, including user data, user settings, and application settings.
- Determine where to store the data while you perform the image-based installation.
- Create a schedule for migrating data on each of your destination computers.
- Describe how to collect and restore the data.

Microsoft provides two tools for migrating user data and settings. Each tool is designed for different types of users and environments.

- **Files and Settings Transfer Wizard.** Designed for home users and small office users. The 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.
- **User State Migration Tool.** Designed for IT administrators who perform large deployments of Windows XP Professional in a corporate environment, the User State Migration Tool provides the same functionality as the wizard, but on a large scale targeted at migrating multiple users. The User State Migration Tool gives administrators command-line precision for customizing specific settings, such as unique modifications to the registry. The User State Migration Tool is located in the `\valueadd\msft\usmt\` folder on the Windows Server 2003 CD.

For more information about migrating user data and settings, see “Migrating User State” in this book. Also see the articles “User State Migration in Windows XP,” “Step-by-Step Guide to Migrating Files and Settings,” “Deploying Windows XP Part I: Planning,” and “Deploying Windows XP Part II: Implementing.” To find these articles, see the Microsoft TechNet link on the Web Resources page <http://www.microsoft.com/windows/reskits/webresources>.



#### Note

You might not need to backup user data if you use folder redirection and roaming profiles to store user data and configuration settings on a server. For an overview of Group Policy and information about using folder redirection and roaming user profiles, 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>).

## Obtaining Client Computer UUIDs

During the auditing process, you can also obtain the UUIDs for your existing client computers. You need the IDs for existing clients that you are planning to prestage in Active Directory to enhance the security of RIS installations. For more information about obtaining UUIDs for prestaging your client computers, see “Evaluating the RIS Client Prestaging Process” later in this section.

Some of your clients, such as those which are not PXE-enabled, might not provide a UUID. For these clients, you need to use the RIS boot floppy disk. After using the RIS boot floppy disk to initiate startup on these clients, Remote Installation automatically generates UUIDs and computer accounts for these clients based on the MAC address of the network adapter.

## Evaluating the Creation of UUIDs for Non PXE-Enabled Clients

When a PXE-enabled client prestaged in Active Directory connects to a RIS server, the UUID of the client computer is passed to the RIS server. The UUID is a unique 32 character hexadecimal or 16-byte number, which is stored with the computer account object that you create in Active Directory. To generate a UUID for these computers, the Remote Installation Services uses the media access control (MAC) address of the network adapter, which is 12 characters long, and prepends 20 zeroes to create a unique 32 character hexadecimal or 16-byte number. After this occurs, Remote Installation creates a new computer account object in Active Directory and associates this unique 32-bit number with the account. Because the MAC address of a network adapter is unique on the network, so is the 32 character hexadecimal or 16-byte identifying number and the computer account as well.

If you want to enhance security for non PXE-enabled clients, you can stage computer accounts in Active Directory for these clients using a staging script. The staging script uses UUIDs generated by a BIOS information script, which retrieves UUIDs from PXE-enabled client computers, suggests possible UUIDs for non PXE-enabled client computers, and stores this information in an Excel spreadsheet. This script creates UUIDs by using a process similar to the Remote Installation method. To find these scripts, see the Remote Installation Scripts link on the Web Resources page <http://www.microsoft.com/windows/reskits/webresources>. For more information about obtaining UUIDs and staging computer accounts, see “Evaluating the RIS Client Staging Process” later in this chapter.

For this part of your planning process, use job aid “Planning for RIS Clients” (ACIRIS\_01.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning for RIS Clients” on the Web at <http://www.microsoft.com/reskit>) to indicate whether you intend to allow Remote Installation to suggest possible UUIDs and computer accounts or if you want to create UUIDs for non PXE-enabled clients by using the BIOS information script.

---

## Evaluating the RIS Client Staging Process

Staging computer accounts in Active Directory means that you create computer account objects in Active Directory prior to client computer startup, using the UUIDs of the client computers to configure the `netbootMachineFilePath` attribute in each computer object. You also configure the user accounts that will use the client machines by providing them with read, write, and set/change password permissions on the computer account objects. When these clients boot to a RIS server, they send their UUID to the RIS server. The server then checks Active Directory for a UUID that matches the UUID that the client sends to the RIS server. If one is found, the RIS server accepts the request for service from that client. By using the staging process, you can greatly enhance security by causing your RIS server to recognize specific clients only.

If you are not concerned with the security of servicing RIS client requests for operating system installations and you are not planning to provide automated installations, you can bypass the prestaging process. If you decide to prestage your client computers in Active Directory to enhance security or provide automated installations, you need to obtain the UUIDs for client computers so you can provide them during the prestaging process. Prestaging clients in Active Directory assures that the RIS server recognizes service requests from these clients, while ignoring all others (if you configure the RIS server to do so). For more information about prestaging client computers to enhance security, see “Planning RIS Server Security” (ACIRIS\_05.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning RIS Server Security” on the Web at <http://www.microsoft.com/reskit>).

In many cases, you can get an Excel spreadsheet with the UUID information from the OEM supplier of the client computers. If you do not have UUID information from the OEM, you can use the BIOS information script. To find this script, see the Remote Installation Scripts link on the Web Resources page <http://www.microsoft.com/windows/reskits/webresources>). You can use this script to automate the process of obtaining UUIDs of all client computers in the default Active Directory Computers container.

To obtain UUIDs by using the BIOS information script, you must run the script at the command line and use the **getalluuids** command. The script uses ADSI and WMI technologies to return valid UUIDs that you can use to prestage client computers in Active Directory. The script provides usage instructions that explain all the input arguments and commands you must specify.

Alternatively, you can also use SMS to obtain the UUID for a computer or group of computers. To use SMS to identify the UUID of a computer or group of computers, see the documentation provided with SMS.

Once you have the UUIDs for your client computers, you can use them to prestage clients by creating new computer accounts in Active Directory. For procedures to prestage RIS clients using the Active Directory snap-in on a RIS server, see “Remote Installation Services administration overview” in Help and Support Center for Windows Server 2003.

You can automate the prestaging process by using the prestaging script; to find this script, see the Remote Installation Scripts link on the Web Resources page <http://www.microsoft.com/windows/reskits/webresources>). If you have UUID listings on an OEM spreadsheet, you can adapt this information as input data to the script, but you must use the exact same Excel spreadsheet format that BIOS information script creates. Otherwise, use the BIOS information script with the `/ExcelPath:` option to print the UUIDs to an Excel spreadsheet for the data you need as input to the prestaging script. For more information about designing Active Directory support, including prestaging RIS clients in Active Directory and automating the prestaging process by using scripts, see “Designing the Active Directory Infrastructure” later in this chapter.

For this part of your planning process, use job aid “Planning for RIS Clients” (ACIRIS\_01.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning for RIS Clients” on the Web at <http://www.microsoft.com/reskit>) to indicate your decision to prestage client computers in Active Directory. Also specify the method you intend to use to obtain the UUIDs and the personnel assigned to the task.

## Evaluating Operating System Configurations

To determine the configurations in which to deploy operating systems to your RIS clients, you need to determine what operating system image configurations you need in your organization. To do this, you need to assess user needs for the following:

- Operating systems
- Desktop configurations
- Drivers and applications
- Computer workstation types, such as desktop or portable computer
- User requirements
- Server components

Completing this evaluation also helps you define the type of installations you require, such as:

- Single-image or multiple-image
- Risetup and Riprep images
- Interactive or fully automated modes

In this part of your planning process, use job aid “Planning for RIS Clients” (ACIRIS\_01.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning for RIS Clients” on the Web at <http://www.microsoft.com/reskit>) to define your operating system configurations and installation types.

### Operating Systems

The primary decision you need to make is how many different client operating system installation choices you need to provide to your RIS clients. RIS can support installations of Windows XP Professional, the Windows Server 2003 Family, Windows 2000 Professional, and Windows 2000 Server. For each operating system you provide, you need to generate a separate image. This can be a file-system-based image generated from your master computer with Riprep, or a CD-based image that you create in a distribution share on the RIS server using Risetup. In both cases, you might also want to create different versions of each image to include certain applications, tools, and drivers for specific RIS clients, or special desktops in the case of Riprep images. The methods for creating custom images are different for Riprep.exe and Risetup.exe. Also keep in mind that each different operating system configuration you choose is another image you must create and maintain.

For information about Riprep and creating master computer installations see “Design a Riprep-Based Installation” later in this chapter. For information about Risetup and creating a CD-based image for a distribution share, see “Design a Risetup-Based Installation” later in this chapter.

## Desktop Configurations

The number of desktop configurations you need depends on the desktop configurations you require for new client computers and the types of existing client desktops you already have (see “Auditing Existing Clients” earlier in this chapter). You can apply a new standard desktop configuration or an existing desktop configuration type to client computers throughout your organization. However, the number of different desktops you plan on making available to RIS clients, along with other components, dictates the number of different operating system images you need to generate and maintain. To make a particular desktop configuration available to RIS clients, you must install an operating system on the master computer, configure the desktop as you want it, and run Riprep.exe on the master computer to create the image and store it on the RIS server. The image on the server then contains the desktop configuration that you configured on the master computer.



### Note

You cannot customize desktops using Risetup images.

## Drivers and Applications

If you need to provide custom drivers, applications, or support files to your RIS clients, you can use Riprep.exe to generate a file-system-based image from a master computer that you configure with the drivers, applications, and Help or support files you need. The most efficient way to provide specific application configurations to users is to prestage a large number of applications on the master computer and create different answer files for each application configuration. For more information about creating your master computer configuration, see “Configuring a Master Installation” later in this chapter.

You can also provide custom drivers and applications to your clients with CD-based images you create using Risetup.exe. After creating the Risetup image on the RIS server, you can do this by:

- Populating the distribution share with the specific drivers and applications your users need — this can include hardware device drivers, such as drivers for storage and Plug and Play devices.
- Modifying the answer file that the installation uses.

## Workstation Types

The types of computers you want to receive RIS-based operating system installations, such as desktops or portables, can impact the operating system configurations you provide. You might want to provide different applications, drivers, and desktop configurations to each of these clients. For example, you might need to provide remote access and a unique suite of applications for your portable computer configurations. You might also need to provide display resolution settings for portable computers.



## User Requirements

You need to identify the requirements of your users so you can define the types of users you have. Obtaining this information is important because it helps you decide how to customize your RIS-based installation design. For example, if a particular group of users needs a specific application, you must add it to the distribution share on your RIS server or configure it on the master computer from which you create a Riprep image.

You can classify user types based on criteria such as the following:

- Computer knowledge — such as beginner, intermediate, or advanced.
- Location — such as on-site, roaming, or remote.
- Job function — such as marketing, research, or customer service.
- Job category — such as manager, project lead, or individual contributor.

As an example, suppose that you classify certain users into types according to computer knowledge. This has an impact on what operating system installation choices you make available to these users. You want to allow less knowledgeable, task-oriented users to make few or no installation choices, while more advanced users might have several installation options from which to choose. To accommodate these differences, you control the configuration of the CIW using Group Policy settings to allow or disallow specific operating system installation options.

User requirements can also include such things as local account passwords, language needs, regional considerations, desktop configurations, and applications such as line-of-business, spreadsheets, and word processing. You can customize user parameters and application configurations in the manner described in “Evaluating Operating System Configurations” earlier in this chapter.

## Server Components

The components you need to provide with a Windows Server 2003 installation can vary, depending on the member server roles you need to provide. If you have several member server component configurations, you can associate multiple answer files with a single CD-based image of Windows Server 2003. For each CD-based image that you create using Risetup.exe, RIS creates a default answer file called Ristndrd.sif. By providing a modified version of this answer file to represent each member server configuration, you can offer a variety of unattended Windows Server 2003 installation configurations from the same source image on the RIS server. This way, you do not have to create additional images to provide different member server component configurations.

You can provide the server components by adding them to the distribution share you create after running Risetup.exe. You can add applications such as IIS, Telnet Services, or Exchange. You then need to configure various parameters for the operating system and server components using the unattended answer file associated with the Risetup image on the distribution share.

## Evaluating RIS Server Requirements

To create a RIS server in your organization, you need to add the Remote Installation Services component to a computer running Windows Server 2003. You can do this in **Control Panel** under **Add or Remove Programs**. You must also configure your RIS server using *Risetup.exe* and you must create at least one operating system image on the server.

You create a RIS server in the deployment phase of your RIS deployment process, but you need to do some preliminary analysis in the planning stage to assure good performance. As part of the planning process, you need to evaluate the following elements to ensure that your RIS server meets the necessary specifications:

- Hardware requirements
- Software requirements
- Server placement
- Server performance

In this part of your planning process, use job aid “Planning for RIS Servers” (ACIRIS\_02.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning for RIS Servers” on the Web at <http://www.microsoft.com/reskit>) to record your planning decisions. At this point, you can specify which personnel you want to perform the task of creating RIS servers and initial installation images.

---

## Evaluating RIS Server Hardware Requirements

In general, RIS servers must meet the requirements of the product version of the Windows Server 2003 family you install. However, you are encouraged to increase those requirements to more efficiently support RIS image deployment in your organization.

You need to have at least two disk partitions available on the RIS server, one for booting the server operating system and another to contain the directory structure for the client operating system images. You need to allocate an entire separate partition to the RIS server directory tree because you cannot install RIS on the same drive as the system volume. Also, you need to format the RIS partition as NTFS.

The partition containing the images must be large enough to store one or more operating system images, depending on your requirements. A CD-based image for Windows XP Professional is 650 MB–700 MB in size. Most organizations store more than one operating system image to meet the needs of different clients.

For up-to-date hardware compatibility information, see the Windows Catalog link on the Web Resources page at: <http://www.microsoft.com/windows/reskits/webresources>.

For this part of your planning process, use job aid “Planning for RIS Servers” (ACIRIS\_02.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning for RIS Servers” on the Web at <http://www.microsoft.com/reskit>) to record whether you require an upgrade to RIS server hardware. Also indicate the personnel you want to assign to the task.

## Assessing RIS Server Software Requirements

Several software components are necessary to support the functioning of a RIS server in your network. You need to verify whether the Active Directory, DNS, DHCP services exist on your network before deploying RIS in your organization. You can find all of these services, including the RIS component, on a server running Windows Server 2003. However, you might also have the DNS or DHCP services provided by a third party. In any case, to assure that you do not have any performance degradation in your production environment, install these services on different servers and configure each server for the specific role of that service.



### Note

You can install all of these software components on a single RIS server when you create your test environment, as discussed in “Designing a Test RIS Environment” later in this chapter.

### Remote Installation Services (RIS)

RIS is an optional component of Windows Server 2003 that provides the services that enable you to automate the remote installation of an operating system, such as Windows XP Professional, on client computers in your organization.

### Domain Name System (DNS)

RIS servers rely on DNS to locate the required Active Directory servers to facilitate domain operations. If you use Windows Server 2003 DNS, you have the benefit of dynamic updates for your DNS server. However, it is not a requirement to use Windows Server 2003 DNS for RIS to function. Whichever DNS server you use, it must support the SRV RR record type and the dynamic update protocol specified in RFCs 2052 and 2136, respectively. For more information about DNS, see “Deploying DNS” in *Designing Network Services* of this kit.

### Dynamic Host Configuration Protocol (DHCP)

RIS servers require a DHCP server on the network which is authorized and has an activated scope. Remote boot-enabled clients must receive an IP address from a DHCP server before they can contact a RIS server to request an operating system installation. You can install Windows Server 2003 DHCP or you can use existing DHCP services provided with Windows 2000 Server. In addition, you can use a third party DHCP server. For more information about Dynamic Host Configuration Protocol (DHCP), 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>).

### Active Directory

You must install RIS on a computer running Windows Server 2003 in an Active Directory domain. For best results, configure this computer as a member server. Although you can install RIS on a domain controller, the heavy traffic load generated by RIS can impact the performance of the domain controller.

RIS uses Active Directory to locate RIS clients and other RIS servers. You can administer the RIS server from the Active Directory Users and Computers snap-in (dsa.msc) located on the RIS server. 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>).

For this part of your planning process, use job aid “Planning for RIS Servers” (ACIRIS\_02.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning for RIS Servers” on the Web at <http://www.microsoft.com/reskit>) to indicate whether you need to verify the existence of the software components required to support RIS, along with the personnel you want to assign to this task.

---

## Assessing RIS Server Placement

In the test environment that you use to test RIS features, RIS performance, and the installation process, RIS server placement is not critical. For example, you can place the RIS server and other supporting components, such as Active Directory, DNS, and DHCP all on a single server. For more information about creating a RIS test environment, see “Designing a Test RIS Environment” later in this chapter.

In the production environment of a large organization, an all-in-one configuration is not recommended because high RIS traffic volumes can cause significant performance degradation in other services on the server that hosts RIS. This can occur when Server Message Block (SMB) traffic from the server to numerous clients in the setup process precludes other traffic on the network. This results in inhibiting DHCP traffic, new PXE requests, other TCP/IP network traffic, and even some Active Directory replication modes. When the performance of DHCP degrades, this can slow the network or even bring it down. For these reasons, avoid configuring production domain controllers with multiple roles that include RIS, Active Directory, DNS, and DHCP.

To assure adequate performance in a large organization, consider using separate computers in your production environment for the following components:

- Domain controller with Active Directory and DHCP
- DNS
- RIS server

In relatively small organizations, placing your DHCP and RIS servers on the same computer is a common practice and works well in most situations. However, you need to be aware that whenever your RIS server approaches its maximum capacity to handle PXE requests, you might begin to see a failure in the ability of your DHCP server to service client DHCP requests. For further information about combining DHCP and RIS, see “DHCP and RIS Server Considerations” later in this section.

Also observe the following guidelines when placing your RIS server(s) in the production environment:

- Do not place RIS on the same computer that is running Exchange Server or Microsoft® SQL Server™.

The high traffic levels of RIS can degrade the performance of these products, and vice versa.

- You cannot host RIS on a computer in a wireless network.
- Do integrate RIS into networks with preexisting third party remote installation servers.

RIS technology allows the coexistence of remote installation servers from multiple vendors on the same physical network. When you set RIS servers to ignore boot requests from unknown clients, you can introduce them on a network without interfering with preexisting remote installation servers that use the same remote boot protocols.

### DHCP and RIS Server Considerations

Because PXE-enabled RIS clients use the DHCP discovery mechanism to obtain a network (IP) address and to locate RIS servers, the relationship of RIS to DHCP in your organization can play a key role in determining your RIS server placement strategy.

In simple environments, a common solution is to add RIS to each DHCP server in use. When you use a combination Windows Server 2003 DHCP/RIS server approach, this reduces the number of initial network packets that RIS clients send to the DHCP and RIS servers. This also increases the server's initial response time. In addition, combining a Windows Server 2003 DHCP and RIS server provides simultaneous answering of client requests. This creates a simplified form of load balancing, because it takes advantage of existing groupings of client computers associated with the DHCP server. This configuration also simplifies troubleshooting and administrative procedures.



#### Important

If the RIS server and DHCP server coexist on the same computer and the RIS server becomes too busy to answer PXE requests, then the DHCP server also becomes too busy and cannot answer IP address requests. However, this issue might be significant only in relatively large organizations.

Because RIS servers can generate large network loads, they often require high-end hardware and usually must be located near the clients they service. By contrast, a DHCP server generates far less traffic, does not typically require high-end server hardware, and is often centralized rather than near client computers. In a centralized configuration, you might find it impractical to simply add RIS to your existing DHCP servers. In such cases, consider adding RIS services to existing software installation point servers, because they have planning and placement requirements similar to RIS servers.

Also, because the PXE-based remote boot process does not provide a way to determine from which RIS server a client receives service, you need to control which RIS server answers specific clients. This is a primary issue when RIS servers are separate from DHCP servers, or when DHCP servers that are not running Windows Server 2003 are in use. In this situation, the location of RIS clients can have an impact on how you configure RIS server selection and load balancing, and subsequently on where you place a RIS server.

### **RIS Server Selection and Load Balancing**

By default, when a PXE-enabled RIS client broadcasts a request for service, all RIS servers receiving the request initiate a reply. The first RIS server on the network from which the client receives a response is the one that provides service to the client. However, combined DHCP/RIS servers have response priority over servers hosting these applications separately. Although this provides a simple form of load balancing among multiple RIS servers available to clients, it is better to balance the load by explicitly restricting which servers can respond to specific clients. This also allows you to prevent specific clients from using RIS servers that you do not intend them to use.

To control server selection, you can physically control network routing so that DHCP discovery broadcasts are forwarded only when appropriate. For example, you might want to forward DHCP broadcasts when a server local to a client is busy or down when the client requests service. By using forwarding to control the routing to a DHCP/RIS server, you can allow answers from only those RIS servers that you configure to receive forwarded client requests.

Another way to control server selection is to configure clients that you prestage in Active Directory to only use a specific RIS server. When a RIS server answers a service request from a client, the server checks the Active Directory forest for the UUID configured in the client computer account to verify whether there is a match to the UUID submitted with the service request. If the RIS server finds a matching computer account, it also checks the account to confirm whether it is configured to use a specific RIS server. If the account designates that only a specific RIS server can provide service, then this is the server that services the client request. The RIS server initially processing the client request then points the client to the RIS server that actually provides the requested RIS services. This is known as a *server referral*. You can use this mechanism as a simple way to control which RIS servers offer operating system installation services to specific client computers.

For information about combining prestagging and referral capabilities to enhance flexibility and security, see “RIS Server Configuration Design Tasks” later in this chapter.

At this point in your planning process, use job aid “Planning for RIS Servers” (ACIRIS\_02.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning for RIS Servers” on the Web at <http://www.microsoft.com/reskit>) to specify the server/software configuration you want to use. Also record the method you intend to use to load balance client service requests to RIS servers (either by configuring routing or using RIS referral servers) and the personnel you want to assign to the task.

## Network Load Considerations

Because RIS servers install operating system images on client computers, the amount of traffic the server produces is similar to that of other servers performing as software installation points on your network. However, the amount of RIS server traffic is more predictable than traffic from a general purpose software installation point that provides applications and regular updates. For example, RIS traffic increases when many users are loading images, during deployment of a new operating system or when you add new computers to the network, and decreases after the initial installations are complete.

To accommodate the periodic high traffic volumes that a RIS server generates, you need to place the RIS server in a location that minimizes its impact across your network. In general, place a RIS server near the client computers it services. This localizes the traffic and reduces its impact during times when multiple image downloads occur. If you have an environment in which re-installations occur frequently, you might consider segmenting the physical network to isolate the RIS server and dedicate it to client installations on that segment.

If you have an environment in which you perform a large number of operating system pre-installations before delivery to clients, consider implementing a RIS-based preinstallation lab. A lab such as this allows you to process a high volume of computers by using high-speed networking to reduce installation times. This also avoids any impact on network performance, because you do not have to place your RIS server on the network at all.

For this part of your planning process, use job aid “Planning for RIS Servers” (ACIRIS\_02.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning for RIS Servers” on the Web at <http://www.microsoft.com/reskit>) to indicate whether you plan to:

- Add your RIS servers to existing software installation points, or DHCP servers.
- Create a preinstallation lab for RIS servers.

If you choose to create a preinstallation lab, record the personnel that you assign to the task.

---

## Planning RIS Server Performance

To plan for the needs of your RIS server, you can assess RIS server performance in your test environment prior to deploying RIS in your network. The results you obtain provide some initial performance indications that can assist you in deciding where to make necessary improvements to the RIS server configuration.

To determine if you need improvements to enhance RIS server performance, you might first analyze the areas in which potential performance bottlenecks can occur. Doing this in your RIS test environment is beneficial for a baseline performance assessment, because the environment uses multiple server roles on the computer hosting RIS. However, for more definitive assessments, you can monitor performance in your actual environment during times of high demand on your RIS servers.

For more information about the RIS test environment, see “Creating a RIS Test Environment” later in this chapter.

Because RIS primarily uses a file-copy process, RIS server performance factors are common to those of other file input/output (I/O) intensive servers, such as Web, file, and print servers. These performance factors include server throughput, disk throughput, and network speed. When a RIS server or its network connection overloads, the result is increased installation time on client computers and TFTP time-outs during the initial file-copy phase.

For this part of your planning process, use job aid “Planning for RIS Servers” (ACIRIS\_02.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning for RIS Servers” on the Web at <http://www.microsoft.com/reskit>) to indicate whether you plan to use the test or production environment to obtain RIS server performance indications.

## Performance Bottlenecks

A *bottleneck* is the part of a computer system that restricts workflow. Generally, a bottleneck is caused by over-consumption of a specific resource. Some causes of bottlenecks include:

- Too many active processes that need access to RAM.
- A processor running at a high percentage of utilization.
- A disk controller or drive that is slow when accessing data.

To monitor for bottlenecks, you can use the Performance tool provided with the Windows Server 2003 operating system to determine which system components are having an adverse effect on total I/O throughput. You can locate the Performance tool on a Windows Server 2003 from the **Start** menu in the **Administrative Tools** group. When you start the tool in MMC, a Help menu item is available to assist you in using the tool.

The components you should consider monitoring include the following:

**Memory.** The best indicator of a memory bottleneck is a sustained high rate of hard page faults. Hard page faults occur when the data a program needs is not found in the working memory visible to the program or elsewhere in physical memory, and must therefore be retrieved from the disk. An acceptable range for this parameter is 0–20 hard page faults per second.

**Processor.** Processor activity is especially important for server-based applications. Two of the most common causes of CPU bottlenecks are CPU-bound applications and excessive interrupts generated by inadequate disk or network subsystem components. Consider processor use in excess of 75 percent to be a bottleneck.

**Disk subsystem.** Just as processor usage is the bottleneck for server applications, the disk subsystem is often the bottleneck for file I/O performance. Because a RIS server is file I/O intensive, disk activity is a primary area to analyze. With the Performance tool, you can evaluate the disk activity of your RIS server in terms of total I/O throughput of the server and percentage use of the disk subsystem.



Table 4.2 describes the Performance tool objects and counters you can use to assess performance of critical systems, including memory, processor, and the disk subsystem.

**Table 4.2 Performance Monitor Objects and Counters**

Object	Counters
Memory	Pages/sec
Processor	% Processor Time
Physical Disk	% Disk Time, Average Disk Queue Length



**Tip**

You can also use the Disk Bytes/Transfer and Disk Bytes/Second counters for the Physical Disk object. High values for these counters indicate efficient use of the disk subsystem, despite heavy disk loads.

Based on the performance monitoring results you obtain, consider making improvements in one or more of the following areas to optimize performance of your RIS servers:

- Increase processor speed.
- Increase the data transmission rate on the network.
- Decrease processor utilization, which can include shutting down unnecessary services on the computer hosting RIS.
- Improve disk utilization.  
Consider providing a disk configuration that uses multiple SCSI II (minimum) hard drives with Redundant Array of Independent Disks (RAID) 5 disk striping with parity.
- Increase the amount of installed RAM.

For this part of your planning process, use job aid “Planning for RIS Servers” (ACIRIS\_02.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning for RIS Servers” on the Web at <http://www.microsoft.com/reskit>) to indicate the components you plan to test (memory, processor, disk subsystem), the potential upgrades you anticipate, and the personnel you want to assign to these tasks.

## Assessing Master Computer Requirements

To plan for your master computer configuration, you need to assess the following:

- Hardware requirements
- Operating system image requirements
- Placement of the master computer

### Master Computer Hardware Requirements

The minimum hardware requirements for your master computer are similar to those of client computers because the master must be capable of supporting the installation of the client's target operating system. This might be an operating system such as Windows XP Professional or Windows Server 2003. For more information about client computer hardware requirements, see "Evaluating RIS Client Hardware" earlier in this chapter.

Because the master computer never participates in remote installations across the network, it is unnecessary for the master computer to be PXE-enabled. However, the master computer must meet the following requirements:

- The HAL must be the same as that of client computers.
- There can be only one disk partition and it must not contain any encrypted files.
- The disk partition size must be less than or equal to the client partition size.

The master computer disk partition contains the operating system and applications you intend to provide to clients. The size of this partition determines the minimum disk size required on client computers that receive the image you create from the master computer using Riprep.exe. During image creation, if a client computer hard disk contains more than one partition, RIS sends a message to the client desktop stating that only the system partition (the one with the Windows folder) will be copied from the master installation image. If the client's boot partition and system partition are different, the computer cannot be imaged.

For this part of your planning process, use job aid "Planning the Master Computer Configuration" (ACIRIS\_03.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see "Planning the Master Computer Configuration" on the Web at <http://www.microsoft.com/reskit>) to indicate whether your master computer requires a hardware upgrade and if you need to verify that the master computer has the following:

- A HAL matching that of client computers receiving a Riprep image.
- A single disk partition the same size (or smaller) than the client computer disk partition, and with no encrypted files.

## Master Operating System Image Requirements

To create installation images of an operating system, run the Riprep wizard on the master computer. When you are ready to create your image, run Riprep.exe from the master computer by specifying the following in the **Run** dialog box:

**\\RISServerName\Reminst\Admin\i386\Riprep.exe**

The master computer contains the operating system, locally-installed applications, and any configured system settings that represent a standard client configuration that you want to deploy. Plan to carefully test each configuration before running Riprep.exe to create the installation image. After Riprep.exe replicates the image to the RIS server, you cannot alter the image configuration without installing the image, making the alterations, and re-running the Riprep wizard to create a new image.



### Note

Overwriting an existing Riprep image on the RIS server is not recommended or supported. It is recommended that you delete the old image and make a new one.

It is likely that you will need to create multiple operating system images from your master computer. When this is the case, consider installing the operating systems you intend to image by using unattended installations. This way, you can create and maintain a separate answer file for each image. This makes it easier to recall the original configurations if you need to make changes. For more information about using unattended installations for your master computer, see “Configuring a Master Installation” later in this chapter.



### Note

At least one Risetup or CD-based image of the master computer operating system must exist on the RIS server.

For this part of your planning process, use job aid “Planning the Master Computer Configuration” (ACIRIS\_03.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning the Master Computer Configuration” on the Web at <http://www.microsoft.com/reskit>) to indicate whether you plan to:

- Install different operating systems on the master computer using unattended answer files.
- Test the master installation prior to running Riprep.exe.

Earlier, in job aid “Planning for RIS Clients” (ACIRIS\_01.doc), you recorded the operating system images you plan to make available to clients, along with application, driver, and desktop configurations.

## Master Computer Placement

If you are placing a RIS server on the network, you might consider placing the master computer in close proximity to the RIS server because you might need to administer the images to create permissions configurations for clients. For more information about specifying security permissions on Riprep images, see “Evaluating Security for Operating System Images” later in this chapter. If you set up a lab for preinstalling and configuring operating system images on client computers prior to delivery to the client, you can place your master computer in any suitable location in the lab.

For this part of your planning process, use job aid “Planning the Master Computer Configuration” (ACIRIS\_03.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning the Master Computer Configuration” on the Web at <http://www.microsoft.com/reskit>) to indicate the location for your master computer, either near your RIS server on the network, or in a lab.

---

## Assess Existing Network Infrastructure

The impact that RIS-based operating system installations have on your network varies with the demand for RIS services. When large scale installations are in progress, your network carries a heavy load because multiple simultaneous operating system image downloads create significant increases in network traffic. For this reason, it is necessary to assess whether your network can support the speed and traffic volumes that permit RIS-based operating system installations in a reasonable amount of time.

To facilitate the assessment of your network, consider drawing a Visio diagram of the network. You can consult Active Directory and your DHCP scopes when determining the organization of the subnets and domains for your diagram.

Use the following guidelines to verify network requirements to support RIS-based operating system installations:

- **Network Topology.** Determine if your network topology can support a data transmission rate of at least 10 megabits per second (Mbps), but preferably 100 Mbps. To support the minimum recommended transmission rate, you need a 10 Mbps Ethernet network with supporting transmission media. For a 100 Mbps transmission rate, you need a minimum of a Fast Ethernet network with Category 5 UTP cable.



### Note

You cannot use RIS on a wireless network.

You also need to determine if the network adapters of your RIS servers and clients can support the minimum data transmission rate.

- **Number of Servers.** Estimate how many RIS servers you need, based on the number of RIS clients in your organization. A single RIS server can use network pipes and allow 75 simultaneous instances of a Riprep or Risetup image to the equivalent number of clients. If you attempt to use a single RIS server to provide service to more than 75 clients, all subsequent PXE client requests for RIS service are ignored. If clients reboot after a TFTP time-out initiated by the RIS server, they are unable to obtain a client connection to that RIS server.



#### Note

The limit of 75 clients per server is based on Microsoft internal testing. Your results might be different depending on your network topology.

- **Firewall.** Assess your need for a firewall. Because PXE does not provide any inherent security mechanisms, ensure that you have a correctly configured firewall for your network to prevent unauthorized access to your RIS server. For more information about RIS server security, see “Planning RIS Server Security” (ACIRIS\_05.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning RIS Server Security” on the Web at <http://www.microsoft.com/reskit>).
- **Disk Image Transfer Time.** You must have a network connection to every RIS client computer. Ethernet local area networks (LANs) and Token Ring LANs are well suited for distributing disk images across a network. Wide area networks (WANs) are generally not fast enough, unless the LAN segments that make up the WAN are connected with a fast T-carrier service (T2 or higher). Digital subscriber line (DSL), cable modem, Integrated Services Digital Network (ISDN), and dial-up modem connections are not suitable for network distribution of RIS images.

Table 4.3 shows connection speeds and image transfer times for various network connections. Image transfer times are based on optimum network speeds only and are calculated for a 2.5 GB disk image. File server performance is not factored into the disk image transfer times. You can use Table 4.3 as a rough guide to help you determine whether your network is a suitable for RIS-based installations.

**Table 4.3 Approximate Image Transfer Times for RIS-Based Installations**

Connection Type	Network Speed	Transfer Time (2.5 GB Disk Image)
Fast Ethernet	100 Mbps	3 minutes, 25 seconds
Fast Token Ring	16 Mbps	21 minutes, 22 seconds
Ethernet	10 Mbps	34 minutes, 9 seconds
T2	6.312 Mbps	54 minutes, 6 seconds
Token Ring	4 Mbps	1 hour, 25 minutes
T1	1.544 Mbps	3 hours, 41 minutes

- **Network Component Requirements.** Your network configuration must include a Windows Server 2003–based server, the DHCP service, DNS, and Active Directory. It is unnecessary for the RIS server to be the sole DNS/DHCP server or the domain controller.

**Note**

It might be necessary to manually add a record to an existing DNS server to allow it to locate a Windows Server 2003–based server where Active Directory is located.

For this part of your planning process, use job aid “Planning the RIS Network Configuration” (ACIRIS\_04.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning the RIS Network Configuration” on the Web at <http://www.microsoft.com/reskit>) to indicate your decisions to:

- Render a network structure diagram.
- Upgrade your network components, including installation and configuration of a firewall.

In the job aid, also record your image transfer time requirements and include the personnel you want to assign to upgrading or other tasks.

Other network-related factors you should evaluate include:

- The network installation point for RIS servers.
- The redirection of RIS client requests.
- The role of routers in forwarding client DHCP requests.

---

## Evaluating Network Installation Points

You need to determine suitable local or remote installation points on the network for each RIS server. It might make sense to have your RIS servers each placed locally in a separate LAN. For example, you might want to isolate the installation traffic by using bridges. If that is the case, make sure all components that redirect network traffic, such as a bridges, switches, hubs, and repeaters, can all support the minimum data transmission rate.

Also, it might be feasible to determine the locations of RIS servers based on the DHCP scopes in your organization. If that is the case, you might place your RIS servers on the DHCP servers throughout your enterprise. For more information about combining RIS and DHCP servers, see “Assessing RIS Server Placement” earlier in this chapter.

If you have a small LAN containing a single subnet and no router, a single RIS server can provide service to all PXE-enabled client computers as long as installation traffic does not exceed network bandwidth and server resource limitations. For routed environments, you can configure prestaged clients with settings that direct them to the nearest RIS server in proximity for service. Also consider having high-speed communication links between routers. In a branch office site connected by a slow WAN communication link, you might place a RIS server at the branch site to avoid overloading the WAN link. Because WAN connections are typically slow, avoid having RIS-based operating system installations cross this type of connection. If they do, RIS server traffic can quickly cause a bottleneck and produce unpredictable results.

For this part of your planning process, use job aid “Planning the RIS Network Configuration” (ACIRIS\_04.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning the RIS Network Configuration” on the Web at <http://www.microsoft.com/reskit>) to indicate the following:

- The number of RIS server installation points you estimate.
- Whether you need to install RIS servers on existing software installation points or on existing DHCP servers.
- Whether RIS servers will be placed either locally or remotely (cross-domain locations with respect to RIS client locations on the network).
- The type of internetworking connection you plan to use for RIS servers.

---

## Redirecting RIS Client Requests

You can perform RIS-based operating system installations across routers and domains. You can also perform RIS installations across Active Directory forests, providing that you configure cross-forest trusts. If you need RIS-based installations to cross routers in your organization, you must determine if your routers must be upgraded to support the data transmission rate. Also, for PXE-enabled clients to contact RIS servers located across routers, you must configure the RIS server IP address in the router IP helper tables. By configuring the router in this manner, a PXE-enabled client that broadcasts an IP address request is redirected to the specific RIS server listed in the DHCP scope. As a result, the client does not need to broadcast another DHCP discover packet to locate a RIS server.

DHCP allows you to configure options 60, 66, and 67 for directing PXE-enabled clients to a RIS server without having to update routers with the IP address of the RIS server. However, for reliable RIS service, avoid this configuration because it is known to not function properly for PXE 1.0 and RIS boot floppy disk clients. This configuration also has other drawbacks.

For more information about using options to redirect PXE-enabled clients, see article Q259670, “Using Dynamic Host Configuration Protocol Options 60, 66, 67 to Direct PXE Clients to RIS Servers May Fail” 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 this part of your planning process, use job aid “Planning the RIS Network Configuration” (ACIRIS\_04.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning the RIS Network Configuration” on the Web at <http://www.microsoft.com/reskit>) to indicate whether you plan to update your router address tables with the IP addresses of RIS servers.

## Forwarding Client DHCP Requests through Routers

Because client service requests are based on the DHCP discovery process, configuring your network to support RIS-based operating system installations across routers has the same requirements as configuring your network to support DHCP across routers.

Routers that you configure to forward DHCP broadcasts also automatically forward client service requests, however, you must ensure that the requests are forwarded to the proper RIS servers in addition to any DHCP servers. Depending on the model in use and the specific configuration, your router might support DHCP broadcast forwarding to a subnet, a specific host, or another router interface. If you use Windows Server 2003 DHCP but you place your RIS servers on separate computers, or if you use a third-party DHCP service, you must ensure that the routers forward DHCP broadcasts to both the DHCP and RIS servers. Otherwise, the client does not receive a reply to its remote boot request.



### Caution

You need to enable DHCP on all routers along all router hops between RIS servers and clients.

For this part of your planning process, use job aid “Planning the RIS Network Configuration” (ACIRIS\_04.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning the RIS Network Configuration” on the Web at <http://www.microsoft.com/reskit>) to indicate whether you plan to configure your routers to forward DHCP broadcast traffic.

---

## Planning RIS Network Security

During RIS-based operating system installations, you need to maintain network security. The elements you need to consider when planning security for your RIS network include those that relate directly to the network, the client, server authorization, and administrative tasks. To plan for securing your RIS server on the network, address the following issues:

- Security risks of your PXE environment.
- NTLM authentication protocol level needed to log on securely over the network.
- Security for non-prestaged RIS clients.
- Enhancement of network security by using prestaged RIS clients.
- Restriction of client installation options.
- Control of the user interaction level during installation.
- Security for operating system images.



- Security for RIS server authorizations.
- Planning security for RIS administrative tasks.

For a job aid to record your planning decisions for RIS server security, see “Planning RIS Server Security” (ACIRIS\_05.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning RIS Server Security” on the Web at <http://www.microsoft.com/reskit>).

---

## Assessing the Security of the PXE Environment

Because of the design of PXE architecture, the PXE environment can introduce some inherent security risks in a network containing a RIS server, as follows:

- PXE has no provisions to detect or prevent unauthorized installations on PXE-enabled client computers from an unknown server. Any server that establishes a connection with a PXE-enabled client can perform an installation on the client computer.
- PXE has no provisions to prevent packet spoofing. As a result, an attacker could send malicious packets to integrate into the client installation.
- PXE cannot prevent unknown PXE-enabled computers on the network from receiving a remote operating system installation from a RIS server.

This last risk is offset by the fact that RIS provides service only to users who log on with valid user credentials. In addition, if you prestage your client computers in Active Directory and configure your RIS server to only respond to known clients, a PXE-enabled intruder gaining access to your network cannot receive an operating system installation or any information about your client computer configurations.

To minimize the potential for successful attacks on your PXE-enabled clients, plan to take the following steps to ensure that unauthorized users cannot connect to them:

- Install and configure a firewall on your network.
- Implement safeguards, such as auditing and monitoring, to detect intrusions on your network.
- Secure physical access to your network.
- Enforce a strict password policy throughout your network.

For this part of your security planning process, use job aid “Planning RIS Server Security” (ACIRIS\_05.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning RIS Server Security” on the Web at <http://www.microsoft.com/reskit>) to indicate the steps you choose to take to secure PXE-enabled clients. Record this information under the section “PXE Environment Security.”

## Evaluating the NTLM Authentication Level

As part of planning for RIS server security, you need to evaluate which level of the NTLM challenge/response authentication protocol you require in your network. RIS can use either of two versions of NTLM to support RIS client network logons, including NTLM (the first version) and NTLMv2. NTLMv2 is inherently more secure than NTLM because of the way it handles encryption keys.

The NTLM version you choose affects the authentication protocol level that clients use, the level at which the protocol negotiates session security, and the authentication level that servers accept. For more information about choosing the most appropriate LAN Manager authentication level in a network that includes RIS, see “Setting the LAN Manager Authentication Level on a network that includes RIS” in Help and Support Center for Windows Server 2003.

When determining the most appropriate version of NTLM for your network, consider the following:

- **The network logon security level you need.** If you choose the highest level of security by using the **Send NTLMv2 response only/refuse LM & NTLM** option, then only NTLMv2 is used. However, when this is the case, you must ensure that all computers involved in the authentication process are running software that supports NTLMv2. If you choose the lower security level by using the **Send NTLM response only** option, NTLMv2 is used wherever possible and NTLM is used only when authenticating computers do not support NTLMv2.
- **The various operating systems you are running.** The NTLM version you choose can affect the ability of Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, and Windows XP Professional computers to communicate with Windows NT 4.0 and earlier clients over the network. For example, Windows NT 4.0 computers earlier than SP4 do not support NTLMv2 and Windows 9x computers do not support any NTLM version.

For this part of your security planning process, use job aid “Planning RIS Server Security” (ACIRIS\_05.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning RIS Server Security” on the Web at <http://www.microsoft.com/reskit>) to indicate the NTLM authentication level you want to use, along with the platforms in use that support the NTLM level you choose. Record this information under the section “NTLM Authentication Level.”

---

## Assessing Security for Non-Prestaged Clients

Providing RIS-based operating system installations to RIS clients that are not prestaged could pose a security risk. To service these clients, you must configure your RIS server to respond to all clients that request service. In this situation, the RIS server does not discriminate between authorized and unauthorized clients making service requests. This could expose your network to malicious clients.

For this part of your planning process, use job aid “Planning RIS Server Security” (ACIRIS\_05.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning RIS Server Security” on the Web at <http://www.microsoft.com/reskit>) to record your choice to configure non-prestaged RIS clients with the right to join the domain or check the box indicating that you will allow Remote Installation to create computer accounts.

---

## Planning for Network Security Enhancement Using Prestaged Clients

You can enhance the security of a network that contains a RIS server by prestaging client computer accounts in Active Directory. By using client computer accounts prestaged in Active Directory and configuring your RIS server to respond only to these known clients, you ensure that unauthorized clients do not receive an operating system installation. You also make sure that the prestaged clients are serviced only by authorized RIS servers.

To prestage client computer accounts in Active Directory, you must obtain the UUID for the client computer and specify it when you create the client computer account. For more information about the requirements for prestaging client computers, see “Evaluating the RIS Client Prestaging Process” earlier in this chapter. For more information about how to prestage client computers, see “Evaluating the RIS Client Prestaging Process” earlier in this chapter and “Designing the Active Directory Infrastructure” later in this chapter.

If you want to optimize security using prestaged RIS clients, plan to do the following:

- Obtain the UUIDs for client computers and prestage client computer accounts in Active Directory.
- Configure users of prestaged client computers with read, write, and set or change password permissions on the prestaged computer account objects.
- Configure your RIS server to only respond to known (prestaged) clients by setting options in RIS server **Properties**.

For more information about how RIS servers respond to prestaged clients, see “RIS Server Configuration Design Tasks” later in this chapter.

For this part of your security planning process, use job aid “Planning RIS Server Security” (ACIRIS\_05.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning RIS Server Security” on the Web at <http://www.microsoft.com/reskit>) to indicate your choices to:

- Enhance security by prestaging client computers in Active Directory.
- Obtain UUIDs for client computers.
- Configure your RIS server to respond to known clients.
- Set user permissions on prestaged computer accounts to enhance security.
- Select the Active Directory domain or organizational unit to which these decisions apply.

## Assessing Security Benefits of Restricting Client Installation Options

To enhance security, you can place restrictions on the client installation process by modifying Group Policy with specific RIS installation options. Group Policy applies to sites, domains, and organizational units. If you have personnel designated to deal with Group Policy issues in your organization, you can flag this as a task they need to perform.

You can use the Group Policy Object Editor MMC snap-in to alter the choices the CIW displays to a particular user or user group. You can configure these choices in the Default Domain Policy or you can create new group policies for specific groups of users that require certain installation options.

If you want to enhance security using Group Policy to modify how the CIW displays installation options to the client, plan to use some of the following RIS-specific Group Policy options:

- **Automatic Setup.** Accommodates an automatic setup process using predefined computer names and locations within Active Directory for client computer accounts. Include this option for client computers you are prestaging in Active Directory to enhance network security or for non-prestaged clients for which you predefine a computer naming format on your RIS server.



### Note

Under this option, if a UUID for a client is not found in Active Directory, the client computer receives a name based on the automatic computer naming format you configure in RIS server **Properties**. Also, the computer account is created in the location you specify in RIS server **Properties**.

- **Custom Setup.** Allows users to define a unique name for their computer and specify where to create the computer account within Active Directory. Include this option for clients you are not prestaging in Active Directory and for client computers that are to be set up by you or someone else during installation. This is a less secure configuration because the RIS server must be configured to recognize any client requesting service. For more information about defining CIW setup options in Group Policy, see “CIW Design Tasks” later in this chapter.
- **Restart Setup.** Allows users to restart an operating system installation attempt if it fails prior to completion. It is best to include this option only with prestaged clients because it is less secure to make multiple installation attempts available to unknown clients.
- **Tools.** Allows users to access tools, including the Recovery Console, from the CIW. Depending on which ISV and OEM tools are installed in your RIS server RemoteInstall share, you might want to limit which RIS clients can access them.

You also need to evaluate whether you want to apply the Group Policy as the default domain policy, or if you need to create new Group Policy objects for particular user groups. These choices are closely associated with how you configure the RIS deployment mode and the CIW. For more information about defining Group Policy, see “Designing for the RIS Deployment Mode” later in this chapter.

For this part of your security planning process, use the “Security Enhancement with Group Policy and User Interaction Level Control” section of job aid “Planning RIS Server Security” (ACIRIS\_05.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning RIS Server Security” on the Web at <http://www.microsoft.com/reskit>) to record your decision to use Group Policy to enhance security. Also indicate if you want to use either the default domain policy or new Group Policy objects. If you plan to use new GPOs, then indicate the user groups where they apply.

---

## Assessing Security Benefits of Controlling the User Interaction Level

You can enhance the level of security in your network by managing client interaction with RIS-based operating system installations. You can predetermine how much user interaction occurs by modifying the CIW configuration. If you want to enhance security by controlling the user interaction level, you might plan to modify the CIW in the following ways:

- Add or remove entire CIW screens.
- Add or remove individual options within CIW screens.
- Provide additional text or instructions to users.
- Create new screens that prompt the user for specific information that you use to control image installation.

For example, you might add a new screen that prompts users to provide additional security information. Also consider that for any entry that you can specify in an answer file, you can create OSC variables in an answer file to capture information that users input in response to CIW prompts. By implementing modifications to the CIW, you can limit the information presented to potential unauthorized clients or require them to provide specific information that ensures they are valid RIS clients. For more information about defining and modifying the CIW configuration, see “CIW Design Tasks” later in this chapter.

You might also consider whether different user groups should receive different modifications to increase the security of RIS installations.

For this part of your security planning process, use the “Security Enhancement with Group Policy and User Interaction Level Control” section in job aid “Planning RIS Server Security” (ACIRIS\_05.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning RIS Server Security” on the Web at <http://www.microsoft.com/reskit>) to record your choice to use the CIW to control the user interaction level. Also indicate the types of controls you want to use and the user groups to which they will be applied.

## Evaluating Security for Operating System Images

As part of planning RIS installation security, you need to evaluate how you intend to control which operating system images you make available to specific RIS clients. If you want to control which clients can access a particular operating system image, plan to do the following:

- Configure user permissions on each image you create, to define which users can install a particular image from the RIS server.
- Remove specific users from the access control list (ACL) on the operating system image folder on your RIS server to prevent these users from viewing (and therefore accessing) the image.

By setting permissions in the ACL of the answer file associated with an operating system image, you can prevent certain users from installing the image. By this means, you can also configure which users can install the image. If you do not set specific permissions on the answer file, then all users can install the image. If you remove a user account (or the group account to which it belongs) from the ACL on the operating system image folder, you disable a user's ability to view an image.

If you intend to use the default answer file with your Riprep or Risetup images, you need to set permissions on the Ristndrd.sif file. Otherwise, you need to set permissions on any custom answer files you create and associate with operating system images you want to configure for access control.



### Note

To enable a RIS user to view and subsequently install an operating system image from the CIW, you need to provide Read permission on both the answer file and the operating system image folder on your RIS server.

For more information about making images available to RIS clients, click the Index button in Help and Support for Windows Server 2003 and in the keyword box type **Remote Installation Services**, then select **Best Practices**.

For this part of your security planning process, use the “Operating System Image Security” section of job aid “Planning RIS Server Security” (ACIRIS\_05.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning RIS Server Security” on the Web at <http://www.microsoft.com/reskit>) to indicate your decision to control access to operating system images by modifying the ACLs of the default or custom answer files. Also indicate whether you want to disable the user capability of viewing and installing an image and the users/groups to which this decision applies.

## Assessing RIS Server Authorization Security

When a RIS server attempts to start on the network, Active Directory checks the RIS server's IP address against a list of authorized RIS servers. If a match is found, the RIS server is authorized to provide service on the network; otherwise, the RIS server is not authorized and cannot answer client service requests.

Part of your planning process for RIS server security involves assessing how you plan to authorize RIS servers on your network. You must authorize every RIS server in Active Directory to prevent unauthorized servers from servicing RIS clients on your network. The factors to consider when assessing the means for authorizing your RIS servers include:

- Who you designate to perform RIS server authorizations.
- Which computer you use to perform authorizations.
- How you perform the authorization of RIS servers.

### Understanding RIS Authorizers

The person who authorizes RIS servers must be logged on as a member of the Enterprise Admins group. You can perform this task as an Administrator, but you might also consider delegating this task to qualified personnel to whom you give Administrative credentials. You might create a special security group to handle this task and add it to the Enterprise Admins group.

For this part of your security planning process, use the "RIS Server Authorization" section in job aid "Planning RIS Server Security" (ACIRIS\_05.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see "Planning RIS Server Security" on the Web at <http://www.microsoft.com/reskit>) to indicate your decision to assign the task of authorization to specific personnel. Also record whether you plan to create a special security group for RIS server authorizers or add the user accounts of authorization personnel to the Enterprise Admins group.

### Understanding RIS Authorization Locations

You can authorize a RIS server from Active Directory Users and Computers MMC snap-in extension (Dsa.msc) on the RIS server itself or you can do so through a server running Windows Server 2003 or Windows XP Professional Remote Desktop session to the RIS server. All the RIS administrative tools, such as the Active Directory extension, are included when you create a RIS server on a computer running Windows Server 2003.



#### Note

In Windows 2000, you can administer a RIS server remotely using a Terminal Session in administration mode.

Alternatively, you can authorize a RIS server from a computer running Windows XP Professional. However, to do this you will need to install the Administrative Tools package on the computer running Windows XP Professional. You can install this package using the `adminpak.msi` application which is located in the `System32` directory of computers running Windows Server 2003.

For this part of your security planning process, use the “RIS Server Authorization” section in job aid “Planning RIS Server Security” (ACIRIS\_05.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning RIS Server Security” on the Web at <http://www.microsoft.com/reskit>) to indicate the authorization location for your RIS servers.

### Understanding RIS Authorization Methods

The methods you can use to perform authorization of a RIS server include using the **Verify** function in RIS server **Properties**, running Risetup at the command line with the /Check argument, or using the DHCP snap-in on a computer running Windows XP Professional. To use the **Verify** function or Risetup at the command line, you must be logged on at the RIS server and belong to the Enterprise Admins group. To use the DHCP snap-in on a computer running Windows XP Professional, you need to install the Administrative Tools package on that computer using the adminpak.msi application.

Note that you use this same DHCP snap-in to authorize DHCP servers. Therefore, if you install RIS on a DHCP server, which is already authorized in Active Directory, it is unnecessary to re-authorize the RIS server.



#### Note

The authorization process does not depend on how you combine or separate RIS and DHCP, nor on whether or not you use Windows Server 2003 DHCP.

For this part of your security planning process, use the “RIS Server Authorization” section in job aid “Planning RIS Server Security” (ACIRIS\_05.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning RIS Server Security” on the Web at <http://www.microsoft.com/reskit>) to indicate the authorization method you plan to use for your RIS servers.

---

### Planning Security for RIS Administrative Tasks

To secure RIS administrative tasks, you need to decide whether you are planning to delegate tasks and then consider the best way to accomplish this securely. Also, you need to seriously consider securing the use of administrator credentials when performing administrative tasks.

For security reasons, when Windows XP Professional Service Pack 1 (SP1) or Windows Server 2003 is installed from the RIS server, the Administrator account is disabled as soon as the client computer is joined to the domain. Also, the Domain Admin group is added to the local computer when it is joined to a domain. If you want to prevent the Administrator account from being disabled when the client computer is joined to a domain, remove the entry DisableAdminAccountOnDomainJoin from the .sif file for that RISetup image.



## Assessing Delegation of RIS Administrative Tasks

If you plan to delegate any RIS administrative tasks, you need to decide how to do this while maintaining security in your network. The best way to delegate RIS administrative tasks is to use existing security groups or define new ones for which you configure the appropriate permissions to perform specific RIS administrative tasks. This allows you to delegate tasks such as managing client installation images, managing prestaged computer accounts, and authorizing and configuring RIS servers.

For example, to install a RIS server and authorize it to Active Directory, the installer must be a member of the Enterprise Admins group. Others, who are responsible for configuring RIS servers and creating installation images, can have user accounts in Enterprise Admins or in another administrative group such as Domain Admins. This ensures they can perform all RIS configuration tasks.

If you have people in your organization who manage accounts and permissions, but do not configure RIS servers or create client installation images, you might make them members of the Account Operators group. You can then grant them folder permissions on the RIS server to perform their management tasks, rather than making them members of the Domain Admins or Enterprise Admins groups. This approach conforms to the best practices principle of granting permissions only where needed.

To set up a new security group for RIS tasks, create an administrative group in Active Directory, add qualified administrative personnel to the group, and then designate the appropriate permissions for RIS tasks. You can set permissions on the RIS server computer account object in Active Directory using the **Remote Install** tab in your RIS server **Properties**.

For more information about permission requirements for RIS tasks, see “Set permissions for administrators who manage client installation images for RIS” in Help and Support Center for Windows Server 2003.

For this part of your security planning process, use the “RIS Administrative Task Security” section of job aid “Planning RIS Server Security” (ACIRIS\_05.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning RIS Server Security” on the Web at <http://www.microsoft.com/reskit>) to record whether you want to delegate RIS administrative tasks and whether you want to use new or existing security groups. You can also specify the personnel to which you delegate the tasks.

## Assessing Security for RIS Administrative Tasks

To minimize security risks, consider not logging on to your computer with administrative credentials to perform RIS administrative tasks. Instead, you and other RIS administrators can log on with a domain user account and use the **Run as** command to accomplish your administrative tasks. For this reason, consider creating alternate user accounts for all your RIS administrators. In addition, strongly consider training all your RIS administrators in the use of the **Run as** command, so they can perform RIS administrative tasks securely.

**Run as** enables you to run various programs and wizards under your administrator account and security context while you are logged on with a different account, such as that of a domain user. This allows you to expose your administrative context only for the specific program you are running and only for the duration of program execution. For more information about the security risks associated with logging on to the network as an administrator, see “Groups and Default Security Settings” in Help and Support Center for Windows Server 2003.



### Note

As a domain administrator, you should seriously consider using **Run as** to accomplish administrative tasks securely. For example, if you run your computer with domain administrator credentials, your Active Directory domain and forest are susceptible to Trojan horses and other attacks that target the logon sequence.

You can access the **Run as** command by using the command line or the user interface:

- **User interface.** In the Windows user interface, you can right-click the executable program (.exe), Control Panel (.cpl) item, or MMC (.msc) console you want to run, then select **Run as** and provide a user account and password.
- **Command-line.** You can use the **runas** command to provide the same capabilities as the “Run as” command in the user interface. For **runas** usage instructions, type the following syntax at the command line (cmd.exe):

```
runas ?
```

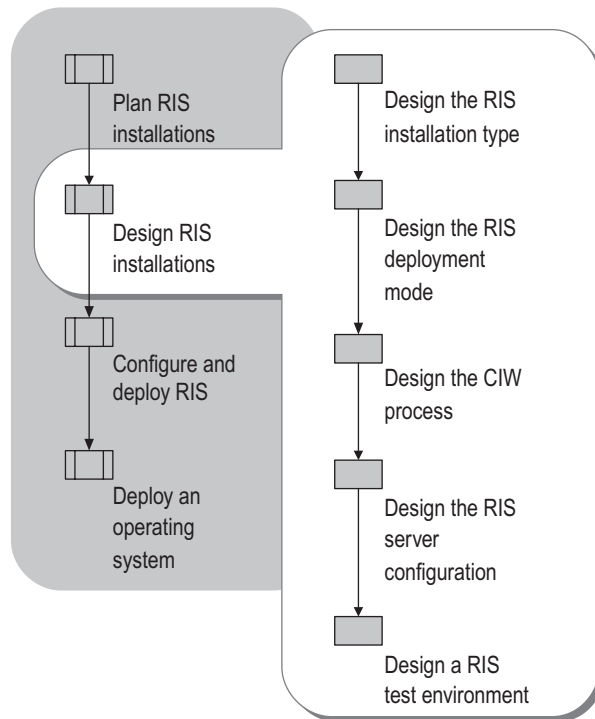
For this part of your security planning process, use the “RIS Administrative Task Security” section of job aid “Planning RIS Server Security” (ACIRIS\_05.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning RIS Server Security” on the Web at <http://www.microsoft.com/reskit>) to record whether you want to:

- Use **Run as** to secure administrative tasks.
- Create alternate domain user accounts or a special group account for RIS Administrators who will use the **Run as** command.
- Train RIS administrators in the use of “Run as.”

# Designing RIS-based Installations

At this point, you can pass your planning job aids to the design team to serve as inputs to the design process. The tasks you must accomplish at this stage of your RIS deployment are illustrated in Figure 4.4.

**Figure 4.4 Designing RIS-based Installations**



## Designing the RIS Installation Type

You can design RIS-based installations using either Riprep or Risetup or both. Riprep installations are based on one or more file system images. Risetup installations are based on one or more distribution folders that contain a CD-like structure for installing the operating system. You can host both Riprep and Risetup images on the same RIS server.

## Design a Riprep-Based Installation

If you are designing a Risetup-based installation, you can skip this section and proceed to “Design a Risetup-Based Installation.”

Use a Riprep-generated image if you want to distribute an image of a fully-configured workstation complete with applications. A Riprep image is essentially a file system image that is located on a remote RIS server. It is similar to the hard disk-images you create using a third-party disk-imaging tool and the Windows System Preparation tool (Sysprep).

You create Riprep images by running the Riprep wizard (Riprep.exe) on a master computer which has the operating system configuration, applications and settings, and desktop customizations you want to deploy to client computers in your organization.

Riprep images are most useful for cloning a standard operating system configuration to clients. Riprep images generally require more disk space on your RIS server than Risetup images because they usually include preconfigured applications and tools. However, they install faster than equivalent size Risetup images.

---

## Riprep Image Design Background

To create a Riprep-based installation, you must first set up a *master installation*. This is the reference computer that contains the operating system, software applications, and configuration settings you plan to install on destination computers in your organization. After you configure the master installation, you run Riprep, which is on the server at the following location:

`\\servername\reminst\admin\i386\riprep`. This converts the master installation into a remote installation image — a functionally identical replica of the master computer disk — that you can install on multiple destination computers. Riprep also replicates the image to a RIS server where it is available for installation on remote-boot-enabled client computers. Clients who request installation of an operating system can access Riprep-based images on a remote RIS server if you configure them to do so.

The best way to install the operating system on your master computer is to use RIS with an unattended installation. For more information about setting up a master installation, see “Configuring a Master Installation” later in this chapter. However, you can also install the operating system locally using the appropriate operating system CD. If you do this, use the disk partitioning utility found on the Windows Server 2003 installation CD and use the text mode setup to clear the disk partition and ensure a clean installation.

After installing the operating system on the master computer, you can install any applications needed by your clients, including line-of-business applications. Before running Riprep to create an image, it is prudent to test the master installation to verify proper configuration and functioning.

Riprep configures various operating system settings on the master computer to ensure that every copy of the master computer's disk image is unique when you install it on destination computers. This includes resetting the security identifiers (SIDs) and ACLs. Riprep also configures the master installation image so that, after the initial installation of the image, every destination computer starts in a special setup mode known as Mini-Setup.

To create a Riprep image from a master installation and store it on a RIS server, your master computer must meet the requirements described in "Assessing Master Computer Requirements" earlier in this chapter. In addition, the following apply:

- You must have at least one Risetup image stored on the RIS server that matches the operating system on the master computer, from where you create the Riprep image.  
The default answer file (Riprep.sif) that Riprep generates for the image refers the client computer to the RIS server to obtain drivers that start the text-mode portion of the CIW during installation of the operating system image.
- The Risetup image on the RIS server must use the same language and have the same first two designations in the version number. For example, a 5.1.2600.0 image will work for a 5.1.2600.1106 version of the same SKU. Only the first two numbers and the SKU type are checked (5.1 Professional) to verify that they are the same as the master computer.
- During image installation, Mini-Setup uses Plug and Play to detect hardware differences between the master and destination computers. Therefore, identical hardware is not needed except for the HAL type. You can only perform a RIS-based installation if the HAL in the RIS (Riprep) image is compatible with the HAL on the destination computer.
- The Riprep wizard only supports preparation and replication of images from the system partition (C:\ *system partition*) on the master computer. The master computer must have a partition no larger than the partition on the destination computer.

In addition, RIS uses the unattended installation process, which means it uses text files, known as setup information (.sif) files, to store the configuration settings for installation images. Each time the client uses the CIW to choose an operating system image, the installation processes the information contained in the .sif file. By modifying the contents of a .sif file associated with an installation image, you can predefine the configuration settings for that image. For more information about software configurations and Risetup images, including modifying answer files, see "Risetup Image Design Tasks" later in this chapter. For more information about defining the CIW configuration, see "CIW Design Tasks" later in this chapter.

## Riprep Image Design Tasks

When designing a Riprep-based installation, your primary tasks are to define how to create and use the master installation. Accomplishing these tasks involves choosing the following:

- The operating systems you want to image.
- The software applications you want to install and configure in the master installation.
- The special hardware drivers you want to include in the master installation.
- Operating system and software settings you want to provide.
- Whether to reuse the master installation to create new images with differing operating system and application configurations. It is not recommended that you reuse the master installation more than two times because Windows Product Activation can only be reset three times.

For a job aid to record your design decisions for Riprep images, see “Defining Riprep Images” (ACIRIS\_06.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Defining Riprep Images” on the Web at <http://www.microsoft.com/reskit>).

### Operating System Images

To begin defining your operating system images, make a copy of job aid “Defining Riprep Images” (ACIRIS\_06.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Defining Riprep Images” on the Web at <http://www.microsoft.com/reskit>) for each operating system you want to deploy. Under “Operating System Image,” create an identifier for each image and enter it under “Image ID Number.” Also enter the product name and the full version number of the operating system for each Riprep image. For Windows Server 2003 and Windows XP Professional operating systems, you can find the version number by viewing the properties of the file Ntdll.dll located in the i386 folder on the operating system CD.

You can locate the version number on the **Version** tab of the **Properties** dialog box. The version number is in the format 5.1.XXXX.Y, where XXXX is the build number. Be sure you include the build number in the worksheet.

### Software Configurations for the Master Installation

Your primary task after installing a master computer operating system is to define which software applications to include in your master installation image. You can use your software inventory in conjunction with the following design guidelines to define a software configuration for each Riprep image you need to create.

**Identify core applications**

Choose the applications you want to include in your master installation image for the client computers and record the application names in job aid “Defining Riprep Images” (ACIRIS\_06.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Defining Riprep Images” on the Web at <http://www.microsoft.com/reskit>) under “Software to Install with This Image.”

**Identify service packs, hotfixes, and patches**

It is a good idea to configure and include service packs, hotfixes, and patches in your master installation images. Because service packs can take a long time to manually install, it is more efficient to include them in the master installation image. Record the names and versions of service packs, hotfixes, and patches under “Operating System Image” in the appropriate copy of job aid “Defining Riprep Images” (ACIRIS\_06.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Defining Riprep Images” on the Web at <http://www.microsoft.com/reskit>) for each operating system image. Keep in mind that if you intend to install any applications after copying a disk image to a destination computer, you might also have to install service packs, hotfixes, and patches after copying the disk image to the destination computer. If you do, record this information under “Software to Install After Image Copy” in each copy you use of job aid “Defining Riprep Images” (ACIRIS\_06.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Defining Riprep Images” on the Web at <http://www.microsoft.com/reskit>).

**Identify applications you cannot install on a master installation image**

In some cases, you must install and configure certain applications only after you copy a disk image to a destination computer. You cannot add applications such as these to a Riprep image. The following are examples of these types of applications:

- Programs that depend on Active Directory, such as Message Queuing (also known as MSMQ) or Microsoft Exchange.
- Special server applications, such as Certificate Services and Cluster service.
- Special applications you want to install only on certain computers.

When you have applications you need to add and configure after installing an image, you might be able to use a Risetup-based installation with an answer file that calls `Cmdlines.txt` or uses the `[GuiRunOnce]` section. For more information about designing a Risetup-based installation, see “Design a Risetup-Based Installation” later in this chapter.

If these methods do not work for your application configuration, you can use Sysprep rather than RIS. With Sysprep, you can stage a group of applications on your master computer and create separate answer files that manage the installation of specific application configurations. For more information about using Sysprep for image-based installations, see “Designing Image-based Installations with Sysprep” in this book.

## Software Application Configurations and Separate Images

When creating Riprep images, it is necessary to create a separate image for each group of computers on which you want a different software configuration. You might need to create separate images when conditions such as the following exist:

- A group of computers requires software applications, utilities, or tools that conflict with software programs required for other computers. For example, you might need to create a separate image for portable computers that require the same vendor-specific programs, such as power-management utilities, DVD codecs, or diagnostic tools.
- A group of computers requires software applications that you cannot automatically install and configure after copying the image to destination computers. For example, you might want to create a separate image for Web servers that all run the same suite of third-party data analysis and monitoring applications. This ensures that all of your Web servers have a consistent configuration and also eliminates the need to manually install and configure third-party applications after you copy an image to a Web server.
- A group of computers requires frequent installation of the same unique software configuration. For example, you might want to create separate disk images for trade-show kiosks or computers that you use for training purposes, because these computers require frequent reinstallation.

For these cases, you can create separate images containing unique application sets. Use job aid “Defining Riprep Images” (ACIRIS\_06.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Defining Riprep Images” on the Web at <http://www.microsoft.com/reskit>) to record your application configurations under “Software to Install with This Image.”

## Hardware Configurations and Separate Images

It is unnecessary to provide separate images for groups of computers on which hardware is detected by Plug and Play. In this case, you do not need to have the same hardware on your destination computers as you configured in your master installation image. However, certain groups of computers in your organization might have special hardware that Plug and Play does not detect. To ensure that the drivers for this hardware are properly detected, you need to add the drivers and any support files to your Riprep image. You can only perform a RIS-based installation if the HAL in the RIS (Riprep) image is compatible with the HAL on the destination computer.

For this part of your Riprep image design process, you need to identify all the unique hardware driver and support files that you need to provide to clients. For each unique configuration, you must create a separate master installation image. You can record the hardware driver and support file information in job aid “Defining Riprep Images” (ACIRIS\_06.doc) (or see “Defining Riprep Images” on the Web at <http://www.microsoft.com/reskit>) on the *Windows Server 2003 Deployment Kit* companion CD under “Hardware Drivers to Install with This Image.”



### Defining the path to special hardware drivers in Riprep answer files

When Plug and Play runs, it enumerates the hardware to get the appropriate IDs and then tries to match the existing hardware with the correct drivers. To find the device driver search path, Plug and Play checks a registry entry that stores the default path to the location of all drivers. The registry entry is **Device Path** in:

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion

The default device path is %windir%\System32\Drivers\. If you have special or legacy hardware that requires drivers that do not exist in the default device path, you can use your riprep.sif answer file to add a new device search path to the registry entry. This enables Mini-Setup (and each subsequent startup sequence of client computers) to find the special hardware drivers.

To add the new device search path to the registry entry, you must specify the entry **OemPnPDriversPath** in the [Unattended] section of the riprep.sif answer file along with the path to the folder containing the drivers. You can include your special drivers, along with any catalog or .inf files, on your system root partition in a folder with a name such as \Drivers.

Riprep prepends %SYSTEMDRIVE% to the folder name, therefore you must ensure that you place your \Drivers folder in the system root partition. Record the special hardware device search path in job aid “Defining Riprep Images” (ACIRIS\_06.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Defining Riprep Images” on the Web at <http://www.microsoft.com/reskit>) under “Special Hardware Driver Path.”

### Defining paths to multiple hardware drivers

If you have different driver types, you can create subfolders under the Drivers folder, which Mini-Setup will automatically search to find all drivers. For example, if you create an Audio subfolder and a Video subfolder, the OemPnPDriversPath entry in your Riprep.sif answer file in the [Unattended] section is as follows:

```
OemPnPDriversPath=Drivers\Audio; Drivers\Video
```

## Operating System and Software Settings

You can configure most operating system and software settings on the master installation before running Riprep. Types of settings you can configure include the following:

- Local policy settings, such as Group Policy Administrative Template settings.
- Control Panel settings, such as power options, sound scheme settings, system startup and recovery options, system performance settings, and accessibility options.
- Internet Explorer settings, such as the default home page, security and privacy settings, and connection settings.
- Optional Windows components settings, such as network monitoring tools, Remote Storage, and Services for NetWare.
- Services settings, such as startup type, logon accounts, and recovery actions.

- Desktop settings, such as desktop shortcuts, folder options, and fonts.
- Display appearance and settings.
- Microsoft Word or Microsoft Excel settings, such as view, edit, save, and spelling options.

For this part of your Riprep image design process, use the “Operating System Settings” section in job aid “Defining Riprep Images” (ACIRIS\_06.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Defining Riprep Images” on the Web at <http://www.microsoft.com/reskit>) to record the settings you intend to include for each master installation image you create.

### Reusing the Master Installation and Windows Product Activation

If you intend to use Riprep images for RIS installations, it is best to use volume license (VL) media for installing your master computer operating system. After running Riprep on a master installation you create with a VL media source, you can reuse the same installation after rebooting and running Mini-Setup, as indicated by the Riprep wizard. At this time, you can install and configure additional applications and run the Riprep wizard on the master installation again. However, if you are unable to use VL media for some reason, ensure that you always clean-install operating systems on the master computer using CD-type images from RIS, or by using a non-VL media CD-ROM. After installing the master computer operating system, you can install and configure applications and run Riprep again.

If you do not have VL media for the Windows XP Professional or Windows Server 2003 operating systems, from which you intend to make Riprep images, you also need to be concerned about Windows Product Activation (WPA). WPA includes an activation timer that is reset each time you create a Riprep image from a master installation configured with a non-VL source. The activation timer controls the grace period during which users must activate their operating systems after installing the Riprep image by using RIS.



#### Note

The activation timer reset behaves similarly on Riprep images that you restore for the purpose of creating a new image.

If you used non-VL media and you attempt to run Riprep on the same master installation more than three times, a warning displays indicating that the activation timer failed to reset. As a result, RIS-based installations of master images of the fourth generation or greater do not have the grace period reset. Therefore, if users install these images after the grace period, they are required to activate Windows at the first logon. If they do not, they are automatically logged out.



#### Note

The WPA issues described here do not apply to flat images that you create with Risetup.

For this part of your Riprep image design process, use the “Operating System Image” section of job aid “Defining Riprep Images” (ACIRIS\_06.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Defining Riprep Images” on the Web at <http://www.microsoft.com/reskit>) to record the media type you intend to use to generate Riprep images.

---

## Riprep Image Design and User Profiles

When designing a Riprep image, be aware that the profile of the user that installs applications and makes configuration changes in the master installation has an impact on the users of client computers where you install the Riprep images. This is a primary concern for the functioning and availability of applications and configurations that are not compliant with Windows Server 2003. For example, some applications might rely upon per-user configurations that are specific to the profile of the user (usually the Administrator) installing the applications prior to running Riprep, rather than to all users of the client computer where the Riprep image is installed.

For this part of the Riprep image design process, use the “User Profiles and Applications” section in job aid “Defining Riprep Images” (ACIRIS\_06.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Defining Riprep Images” on the Web at <http://www.microsoft.com/reskit>) to record any applications included with your Riprep image that are not compatible with Windows Server 2003. Also include the name of the user profile under which you intend to install applications and make configuration changes. For more information about the effect of user profiles on Riprep images, see “Testing Riprep Images and User Profiles” later in this chapter.

---

## Design a Risetup-Based Installation

Risetup allows you to create a CD-type image to be used with RIS installations on client computers. When designing a Risetup-based installation, use the job aid “Planning for RIS Clients” (ACIRIS\_01.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning for RIS Clients” on the Web at <http://www.microsoft.com/reskit>). as input to the design processes outlined in this section.

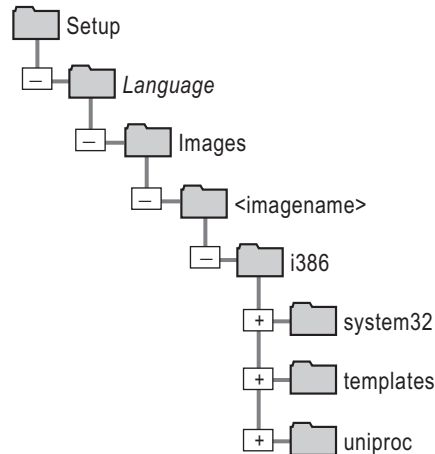
Use a Risetup-generated image if you want to distribute the network equivalent of CD-based installation functionality. A Risetup image is a replica of an operating system CD file structure, located across the network on a remote RIS server.

You create Risetup images by running the Risetup wizard on a RIS server, while using an operating system CD to create the image. When using Risetup images, you cannot provide a fully-configured clone of an operating system with applications and desktop customizations, as you can with Riprep images. However, you can add applications and drivers to the distribution folder where the Risetup images are located and use answer files to install the applications and specify the location of drivers.

## Risetup Image Design Background

Installing a Risetup image is similar to setting up a workstation directly from a CD, however, the source files are located across the network on a RIS server. Figure 4.5 shows the directory structure of your RIS server under the RemoteInstall folder where Risetup images are stored. You can define the name of the folder <imagename> where the images are located.

**Figure 4.5 Directory Location for Risetup Images**



When you install remote installation services on your RIS server, it automatically creates one Risetup image of the server operating system and stores it under the Images folder within the RIS directory structure, as shown in Figure 4.5. This image is available to remote boot enabled clients. Clients that request installation of an operating system can access Risetup images on a remote RIS server, if you configure them to do so.

You can make additional Risetup images using operating system CDs for Windows 2000 Professional, Windows 2000 Server, and Windows 2000 Advanced Server, in addition to Windows XP Professional and Windows Server 2003. To create a Risetup image, place the CD in the CD drive of your RIS server and run the Risetup wizard from the **Images** tab of RIS server **Properties**. You can also specify the following command string at the command line interface to start the Risetup wizard:

```
risetup -add
```

After creating a Risetup image, you can add applications and device drivers located in the RIS server directory structure, as described in “Risetup Image Design Tasks” later in this chapter.

**Note**

The RemoteInstall folder, which is the parent folder of your RIS server directory structure, is shared as Reminst, so that images, applications, and drivers are available to RIS clients on this distribution share.

You can create and associate multiple answer files with Risetup images, which allows you to customize the applications and drivers you want to install with each image. However, you cannot include preconfigured application or desktop configurations with a Risetup image. Also, Risetup images take longer to install than an equivalent size Riprep image.

---

## Risetup Image Design Tasks

When designing a Risetup-based installation, your primary tasks are to choose the following:

- The operating systems you want to image.
- The software applications you want to include on your distribution share.
- The special hardware drivers you want to include on your distribution share.
- The operating system configuration settings or components you want to provide.

For a job aid to record your design decisions for Risetup images, see “Defining Risetup Images” (ACIRIS\_07.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Defining Risetup Images” on the Web at <http://www.microsoft.com/reskit>).

### Operating Systems

To begin defining your operating system images, make a copy of job aid “Defining Risetup Images” (ACIRIS\_07.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Defining Risetup Images” on the Web at <http://www.microsoft.com/reskit>) for each operating system you want to deploy. Under “Operating System Image,” create an identifier for each image and enter it under “Image ID Number.” Also enter the product name and the full version number of the operating system for each Risetup image.

For Windows Server 2003 and Windows XP Professional operating systems, you can find the version number by viewing the properties of the file Ntdll.dll located in the i386 folder on the operating system CD. You can locate the version number on the **Version** tab of the **Properties** dialog box. The version number is in the format 5.1.XXXX.Y, where XXXX is the build number. Be sure you include the build number in the job aid.

## Software Configurations and Risetup Images

In many cases, you can use a modified Ristndrd.sif answer file to automatically install and configure software applications after installing a Risetup image. The answer file provides the information necessary to do this at the end of Mini-Setup or after Mini-Setup finishes, which follows initial image installation on the client. To enable application installation at these times, you need to create an \SOEM\$ folder at the same level as the i386 folder for the appropriate image in your RIS directory structure, and place your applications and related support files in a folder you create with a name such as Applications. The path to such a folder is as follows:

RemoteInstall\Setup\Language\Images\ImageName\SOEM\$\1\Applications

By staging your applications in this location and then using answer files to install the applications on the client, you can minimize the number of images you need to manage and simplify the modification of software configurations as group needs change. However, you need to maintain separate answer files that define the unique application installation configurations. The methods available to define these configurations in your answer files include:

- Pointing to Cmdlines.txt
- Specifying the appropriate entries in the [GuiRunOnce] section

Using these methods enables you to maintain a single image from which you derive multiple application (or driver) configurations that you can provide as installation options to meet varying client needs. You provide these options to the client by associating each answer file with the Risetup image and then configuring access control entries (ACEs) on each answer file to define which clients can receive specific image-answer file sets. For more information about defining operating system installation options, see “Interactive Installation Design Tasks” later in this chapter.



### Note

For application installation, you can also use Group Policy to configure computer or user deployments of applications. For more information about Group Policy-based software deployment, 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>).

If you intend to stage your applications, use job aid “Defining Risetup Images” (ACIRIS\_07.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Defining Risetup Images” on the Web at <http://www.microsoft.com/reskit>) to record your pool of applications under “Applications Staged in \SOEM\$ Folder.” Also, record the staging path to your applications under “Staging Path for Applications,” using the name of the new folder you plan to create to contain them. In addition, use the “Answer File Versions” section of job aid ACIRIS\_07.doc to record your answer file names and software configuration for each answer file. In job aid ACIRIS\_07.doc, you can identify your Risetup answer files with any suitable names, such as Ristndrd01.sif and Ristndrd 02.sif.

To create the answer files, you can copy and modify the default Risetup answer file (Ristndrd.sif) from the following location after you create a Risetup image:

RemoteInstall\Setup\Language\Images\ImageName\i386\Templates\

To create new answer files or to modify existing answer files, you can use Setupmgr.exe or a text editor such as Notepad.

For further information about configuring answer files, see the Deploy.cab file in the \Support\Tools folder on your Windows XP Professional or Windows Server 2003 operating system CD. This file contains a complete reference to the entries you can add or modify for the [Unattended] section. However, be aware that not all sections and entries you find in Deploy.cab apply to RIS.

**Tip**

Consider testing your answer file configurations with an actual operating system installation in your RIS test environment. This ensures proper functioning before performing RIS installations in your production environment.

## Hardware Configurations and Risetup Images

It is unnecessary to create separate answer files that specify installation of hardware drivers for groups of computers on which hardware is automatically detected by Plug and Play. However, you might have special hardware on certain groups of computers in your organization that Plug and Play does not detect. To ensure that the drivers for this hardware are properly detected, you need to add the drivers and any support files to your RIS distribution share in an \SOEM\$ folder you create, and point to this location in your answer files. For storing your driver files, you can create a subfolder with a name such as “Drivers” in the following path within your RIS directory structure:

RemoteInstall\Setup\Language\Images\ImageName\SOEM\$\1\Drivers

**Note**

You can also structure the Drivers folder with subfolders; Mini-Setup searches all the subfolders when attempting to detect drivers for your hardware.

For this part of your Risetup image design process, you need to identify all the unique hardware driver and support files that you want to provide to clients. For each unique configuration, you must create a separate answer file that provides the commands to install the specific drivers. You can record the hardware driver and support file information in job aid “Defining Risetup Images” (ACIRIS\_07.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Defining Risetup Images” on the Web at <http://www.microsoft.com/reskit>) under “Hardware Drivers Staged in \SOEMS\$\1\Drivers Folder.” You can record the answer file names with the hardware driver configurations that they install under “Answer File Versions” in job aid “Defining Risetup Images” (ACIRIS\_07.doc).

**Note**

If you have a large number of special drivers, you can include them all in your Drivers folder. After installing the Risetup image on a group of client computers, you can have your answer file call Cmdlines.txt, which you can preconfigure with commands to remove the unused hardware drivers for that user group.

**Defining the path to special hardware drivers in Risetup answer files**

For special or legacy hardware that requires drivers that Plug and Play cannot detect, you can use your Ristndrd.sif answer file to add a new device search path. This path enables Mini-Setup (and each subsequent Plug and Play detection sequence on client computers) to find the special hardware drivers.

As with Riprep images, you can specify the path to special hardware drivers by including the registry entry **OemPnpDriversPath** in your Ristndrd.sif answer file in the [Unattended] section as follows:

```
OemPnpDriversPath=Drivers\Audio; Drivers\Video
```

For more information about defining the path to special hardware drivers in Riprep answer files, see “Riprep Image Design Tasks” earlier in this chapter.

If you have multiple hardware configurations for different user groups that use the same Risetup image, you can create different answer files with different search paths to the required hardware drivers. In each answer file, add the [Unattended] section and OemPnpDriversPath entries to specify the different paths.

For this part of the image design process, identify the path(s) to your special hardware drivers using the new folder(s) you plan to create, and record this information in job aid “Defining Risetup Images” (ACIRIS\_07.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Defining Risetup Images” on the Web at <http://www.microsoft.com/reskit>) under “Staging Paths for Hardware Drivers.”



## Installing Applications and Drivers

After you install a Risetup image on a client computer, you can install special applications and drivers by calling the Cmdlines.txt file at the end of Mini-Setup or by using [GuiRunOnce] to provide commands that execute after Mini-Setup runs. To set up for application or driver installation, you need to create Cmdlines.txt and configure it with the commands you want to run, or use the [GuiRunOnce] section in your Ristndrd.sif answer file to run the commands that perform the installation.

### Using Cmdlines.txt

Consider using Cmdlines.txt in your Risetup image design when you want to do the following:

- Install applications from the %OEM\$ folder on your RIS distribution share.
- Install applications at the end of Mini-Setup.
- Install an application that is designed for installation by one user, and you need to replicate user-specific information to all users of the computer.

However, before you decide to incorporate Cmdlines.txt into your Risetup image design, consider the following limitations:

- **Logon context.** When Cmdlines.txt is called, it runs as a system service.  
This means there is no logged-on user and no network connectivity. All user-specific information is written to the default user portion of the registry, and all subsequently created users inherit those registry settings.
- **Application support files.** You must place the files necessary for an application or utility to run in your RIS distribution share.
- **Quiet mode.** When you install applications by using Cmdlines.txt, you must install the application with an unattended setup so the user does not need to respond to messages about the application.
- **Limited applications.** You cannot install Windows Installer (.msi) applications with Cmdlines.txt. To install these types of applications, use [GuiRunOnce] instead.

For this part of the image design process, check the “Use Cmdlines.txt” check box in job aid “Defining Risetup Images” (ACIRIS\_07.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Defining Risetup Images” on the Web at <http://www.microsoft.com/reskit>), if you intend to use Cmdlines.txt to install applications or drivers.

**Creating Cmdlines.txt commands**

To use Cmdlines.txt for installing components such as applications and drivers, you first need to create the file and then add the specific command strings that start the installations. You create the Cmdlines.txt file with a text editor such as Notepad (or Setupmgr.exe). In the Cmdlines.txt file, use the following syntax to specify the commands you want to run to install applications or drivers:

```
[Commands]

"command_1"

"command_2"

. . .

"command_x"
```

The command strings enclosed in quotation marks specify the commands that execute in order when Cmdlines.txt is called. For example, you could create a command string to run the commands in an .inf file as follows:

```
"%windir%\System32\Rundll32.exe ApplicationName.inf"
```

When you finish creating Cmdlines.txt, you need to place it in the following path in the RIS server directory structure:

`RemoteInstall\Setup\Language\Images\ImageName\%OEM%\$1\Subfolder`

The folder *Subfolder* might be named Drivers or Applications, as described earlier in this section in the discussion about software configurations and Risetup images. You also need to place the application(s) you want to install (along with any support files) in the \%OEM%\\$1\Application subfolder and the drivers you want to install along with support files in the \%OEM%\\$1\Drivers subfolder. In addition, you must specify the following value in the [Unattended] section in your Ristndrd.sif answer file to point to the location of the applications, special drivers, and Cmdlines.txt:

```
InstallFilePath=RemoteInstall\Setup\Language\Images\ImageName\%OEM%\$1\Subfolder
```

After you properly configure all these parameters, Cmdlines.txt will run automatically at the end of Mini-Setup and process each command that it contains to install the applications you specify.

For this part of your Risetup image design process, record the commands you intend to run in Cmdlines.txt under the “Cmdlines.txt Commands” section of job aid “Defining Risetup Images” (ACIRIS\_07.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Defining Risetup Images” on the Web at <http://www.microsoft.com/reskit>).

### Using GUIRunOnce

Consider using [GuiRunOnce] in your Risetup image design when you want to do the following:

- Install applications or drivers from any source, including network shares, hard disks, or CD-ROM drives.
- Install applications or drivers, but you cannot use Cmdlines.txt; this is the case if you want to install applications that use the Windows Installer (.msi).
- Log on as a user and not automatically replicate application registry settings to future users.
- Require a user to be logged on to the computer when the application or driver installs.
- Control the order in which applications or drivers install.

However, before you decide to incorporate [GuiRunOnce] into your Risetup image design, consider the following restrictions:

- **Enabled log-on function.** [GuiRunOnce] requires enabling the log-on function.

This requires you to set up the automatic logon process by adding the AutoLogon=Yes value in the [Unattended] section in your Ristndrd.sif answer file.

- **Login context.** [GuiRunOnce] commands run in the security context of the currently logged-in user.

If the logged-in user does not have the permissions necessary to run the command completely, then the application fails to install. Because of running in this context rather than as a service, the registry entries that the application creates are for the current user rather than the default user. If you want settings to register only for the currently logged-in user, then [GuiRunOnce] might be appropriate. Otherwise, use Cmdlines.txt to run commands that install applications, because it runs as a system service.

- **Application restarts.** [GuiRunOnce] commands that install applications that force a restart might not complete unless you can suppress the restart.

When a computer restarts, all entries in the [GuiRunOnce] section are lost, meaning that these commands do not execute. If the application does not provide a way to suppress restarts, you might be able to repack the application into a Windows Installer package (.msi) using Veritas WinInstall.

For further information about the 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>).

- **Shell not loaded.** [GuiRunOnce] does not function if an application requires installation of the Windows Explorer shell, because the shell is not loaded at the time GuiRunOnce commands execute.
- **Use of /Wait switch.** [GuiRunOnce] commands often require you to use of the /Wait switch to avoid application setup failures caused by multiple instances of the installation mechanism running.

While Setup is running, initiating a second process and closing an active one might cause the next routine listed in RunOnce registry subkey to start. When this occurs, more than one instance of the installation mechanism is running, which usually causes the second process to fail.

For this part of the image design process, check the “Use GUIRunOnce” check box in job aid “Defining Risetup Images” (ACIRIS\_07.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Defining Risetup Images” on the Web at <http://www.microsoft.com/reskit>), if you intend to use [GUIRunOnce] to install applications or drivers.

### Creating GUIRunOnce commands

The [GuiRunOnce] section of your answer file contains commands that execute the first time users log on to their computers after Mini-Setup completes. To set up this process, each command under [GuiRunOnce] creates an entry in the registry subkey Runonce when your answer file is parsed during image installation. Runonce is located in:

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion.

When the user logs on after Mini-Setup finishes, this registry subkey is checked for any commands that should be executed.

For example, you might start the wizard that installs Active Directory by specifying the following command string in the [GuiRunOnce] section in your Ristndrd.sif answer file:

```
[GuiRunOnce]

"%windir%\system32\dcpromo.exe" /answer:answer_file
```

Note that you must specify each command line in quotation marks under [GUIRunOnce]. Also, the dcpromo command requires an answer file, specified on the command line, to provide input to the wizard.

For this part of your Risetup image design process, record the commands you intend to run under the “[GuiRunOnce] Commands” section of job aid “Defining Risetup Images” (ACIRIS\_07.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Defining Risetup Images” on the Web at <http://www.microsoft.com/reskit>).

For additional information about GUIRunOnce, including controlling application installation, see the Deploy.chm help file in the Support\Tools folder on your Windows XP Professional or Windows Server 2003 operating system CD.



### Important

Deploy.chm and Ref.chm must be in the same directory for Deploy.chm to provide the most complete RIS help information. You can open these files on the operating system CD, or open them on your computer by installing Deploy.cab in a folder on your computer.

## Operating System Settings

You can configure many operating system settings in your Ristndrd.sif answer file. For example, you can use the following entries in the [Components] section in your answer file to determine whether the components associated with these keys will be installed with the operating system:

- Calc
- Certsrv
- Deskpaper
- Fax
- MousePoint
- MSWordpad
- Paint

For this part of your Risetup image design process, record the components or configuration settings you plan to provide using Ristndrd.sif answer files in “Answer File Versions” under “Components/Configuration Settings” in job aid “Defining Risetup Images” (ACIRIS\_07.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Defining Risetup Images” on the Web at <http://www.microsoft.com/reskit>).

For further information about operating system settings you can configure in Ristndrd.sif answer files, see the Reference/Unattend.txt section of the Deploy.chm help file in the \Support\Tools folder on your Windows XP Professional operating system CD.

## Designing the RIS Deployment Mode

You can design your RIS-based operating system deployment to use either the interactive or fully-automated mode. Interactive mode requires the user to respond to predefined options presented during installation at the client computer; the fully-automated mode requires no user intervention other than turning on the client computer and providing logon credentials.

You might want to provide interactive installations for more knowledgeable users who can easily provide the user input you require. For users that are less knowledgeable, you can provide fully-automated installations that require little or no input. This ensures that installation on these clients goes smoothly and does not require your presence at the client computer.

If you want to provide a combination of interactive and fully automated installations to RIS clients, you can prestage your client computer accounts in Active Directory by using the prestaging script along with an input file that specifies which Startrom.com boot file each prestaged client must use. To find the prestaging script, see the Remote Installation Scripts link on the Web Resources page <http://www.microsoft.com/windows/reskits/webresources.>



### Note

The RIS deployment mode design process is closely associated with the CIW design process. For further details, see the job aid “Designing the RIS Deployment Mode and CIW Process” (ACIRIS\_08.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Deployment Mode and CIW Process” on the Web at <http://www.microsoft.com/reskit>).

---

## Interactive Installation Design Background

An interactive installation requires users at client computers to press the F12 key to initiate a network service boot. This occurs automatically when you use the default Startrom.com boot file for RIS installations. After the client initiates the network service boot and obtains an IP address from DHCP, the CIW downloads to the RIS client. At this point, the information gathering and option choosing process of the CIW begins.

You can configure the CIW to display numerous required user input fields on a menu of installation options. You can also configure the CIW to present specific operating system installation options, such as a list of Risetup or Riprep images. These capabilities enable you to control the user input necessary to enable the installation and to designate who can access predefined installation configurations.

For example, you might allow one group of users to have access to all predefined operating system installation options, but restrict another group of users to a single installation option. You can achieve this type of control over the installation process by using Group Policy and ACL configuration.

## Interactive Installation Design Tasks

When designing an interactive installation, your primary tasks are to choose the following:

- The information you require users to input to the CIW.
- The operating system installation options you want to make available to different users via the CIW.
- Which users receive specific RIS setup options that you configure in Group Policy.

For a job aid to record your design decisions for an interactive installation, see “Designing the RIS Deployment Mode and CIW Process” (ACIRIS\_08.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Deployment Mode and CIW Process” on the Web at <http://www.microsoft.com/reskit>).

### Defining User Input

You can configure the user information that is required as input to the CIW. For example, the first screen presented by the CIW is the Welcome screen. You can modify this screen to include multilanguage choices or additional information such as a company message. The next screen is the Logon screen, which requires the user to provide logon credentials, including user name, password, and domain name. You can also build custom CIW screens to prompt the user for specific input information. For more information about defining the CIW configuration, including customizing CIW screens with language options and input prompts, see “CIW Design Tasks” later in this chapter.

At this point in your interactive installation design process, you might need to further analyze your user input requirements. If this is the case, you can wait until you review the section “Designing the CIW Process” later in this chapter before recording your design decisions. Otherwise, use the “Required User Input” section of job aid “Designing the RIS Deployment Mode and CIW Process” (ACIRIS\_08.doc) to record the choices you make for required user input. You can also specify the users or user groups from which you require the input, under “Applicable User Groups.”

### Defining Operating System Installation Options

You can define which operating system images the CIW allows specific users to install, and you can limit the images the CIW displays to specific users by configuring ACLs. By providing ACEs on the answer files associated with a RIS installation image and by providing ACEs on the RIS server operating system image folder, you can determine which clients get to view and install a particular image.

For example, to enable a particular user group to install a RIS image, you must configure the group with Read permissions on the answer file and Read permissions on applicable RIS server operating system image folder. This causes the operating system images associated with that answer file to display in the CIW as installation options for the user group. If you specify Read permissions only on the answer file and not on the image folder, the option to install the image displays in the CIW, however, the image does not install due to the lack of Read permissions on the image folder. When configuring ACEs on the operating system image folder on your RIS server, use the following directory path:

`\\RISServerName\RemoteInstall\Setup\Language\Images\ImageName\`

You can also set an answer file permission configuration to Deny Read access to a particular user group. This causes all operating system images associated with that answer file to *not* display in the CIW as installation options for that user group.

When enabling access to operating system images, you will probably want to simplify administration. Therefore, the best approach might be to enable Read permissions for all users on the image folder and then use answer files to provide Read permissions to specific user groups. However, note that by configuring ACEs on the image folder, you can explicitly prevent certain users and groups from being able to view an installation option for a particular operating system image located on your RIS server.

For this part of your interactive installation design process, use job aid “Designing the RIS Deployment Mode and CIW Process” (ACIRIS\_08.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Deployment Mode and CIW Process” on the Web at <http://www.microsoft.com/reskit>) to record your choices for the operating system installation options you want to provide, along with the user groups that can or cannot receive them. In this job aid, you can specify the following under the “Operating System Installation Access” section:

- Answer file name.
- Operating system image associated with the answer file.
- Users or groups of users granted or denied access to operating system images based on the answer file ACL.
- Users or user groups denied access to specific images based on the image folder ACL.

If you need to record this information for multiple operating system images, make an additional copy of the job aid for each operating system image. You might also make more copies of this job aid for recording information that applies to automated installations.



## Defining Installation Options with Group Policy

You can use Group Policy to configure certain installation options presented by the CIW. With Group Policy, you can create different Group Policy objects to apply to specific users and configure each policy with settings such as **Automatic Setup**, **Custom Setup**, **Restart Setup**, and **Tools**. Each of these options has three different settings associated with it: Enabled, Disabled, and Not Configured.

For example, you could create a separate Group Policy object that provides the **Automatic Setup** option. This causes the CIW to present the appropriate options for clients you have prestaged in Active Directory or for non-prestaged clients that receive predefined computer account names and locations from your RIS server. For non-prestaged clients, you can also create a separate Group Policy object that configures the **Custom Setup** option. This option allows the client to override the automatic computer naming format and causes the CIW to present options to these clients that allow them to specify computer names and the location for their computer accounts in Active Directory.

You can also enable the **Restart Setup** option to allow certain user groups to restart a failed operating system installation attempt if the failure occurs during the text-mode portion of the setup process. This might be useful for security purposes. Also, you can enable the Tools option from Group Policy to allow certain user groups to have access to maintenance and troubleshooting tools for client computers, including the Recovery Console.



### Note

If you specify Not Configured for a particular RIS setting in a Group Policy object that you define, the default Domain Group Policy setting for the associated option applies.

You can also use the RIS-related Group Policy capabilities to improve security in your network. For more information about the security implications of Group Policy as well as ACL settings, see “Planning RIS Server Security” (ACIRIS\_05.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning RIS Server Security” on the Web at <http://www.microsoft.com/reskit>). For more information about defining CIW setup options in Group Policy, including Group Policy options, see “CIW Design Tasks” later in this chapter.

For this part of your interactive installation design process, use the “Group Policy Configuration” section of job aid “Designing the RIS Deployment Mode and CIW Process” (ACIRIS\_08.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Deployment Mode and CIW Process” on the Web at <http://www.microsoft.com/reskit>) to record your choices for RIS-related Group Policy settings. In this job aid, you can record Group Policy names, the configuration options you want to set, and the user groups to which they apply.

## Fully-Automated Installation Design Background

You can design your RIS installation to occur in the fully-automated mode, so that no user input is necessary other than logon credentials. To automate installations on remote boot enabled clients, you can use the alternate RIS boot file `Startrom.n12` to automatically start downloading the CIW after the RIS client successfully accesses a RIS server. When this occurs, the user initiating the RIS installation does not receive a prompt to press the F12 key for a PXE boot. Instead, the fully automated installation of `Risetup` or `Riprep` images proceeds silently after the user logs on.

To enable a fully automated RIS-based installation, it is necessary to substitute the `Startrom.n12` boot file for the default `Startrom.com` boot file. There are two different ways of doing this, depending on the configuration you want:

### Rename the files

To configure all clients serviced by a RIS server with an automated installation, rename the startup boot files as follows:

- Change `Startrom.com` to `Startrom.bak`
- Change `Startrom.n12` to `Startrom.com`

These files are located in the following directory location on your RIS server:

`RemoteInstall\OSChooser\i386`

You can change the names of the startup boot files manually or you can do this remotely from any computer in the RIS domain by using the change boot file script. To find this script, see the Remote Installation Scripts link on the Web Resources page (<http://www.microsoft.com/windows/reskits/webresources>). You can also run this script locally on a RIS server. By specifying the “automated” or “interactive” command arguments with the script, you can toggle the names of the boot files back and forth to support the default interactive mode or the automated mode, as appropriate. Once you configure the names of the boot files, all clients contacting the RIS server receive the same installation mode.

### Assign Startrom.n12 to specific clients

If you want to configure automated installations on certain clients only, you can specifically assign them the Startrom.n12 file as the startup file. However, you only have this level of control by using the prestaging script. This script prestages RIS client computer accounts in Active Directory using an Excel spreadsheet generated by the BIOS information script to provide input data. In the spreadsheet, you can add information to specific data cells to configure which startup file each prestaged RIS client should receive. To find these scripts, see the Remote Installation Scripts link on the Web Resources page

<http://www.microsoft.com/windows/reskits/webresources.>).



#### Important

If you change the name of the startup boot files on a RIS server and you also prestage client computers with specific startup file configurations, client computers might not receive the correct startup file. To avoid this problem, either configure startup files with the prestaging script or change the name of the startup file so all clients contacting the RIS server receive the same boot file. Do not use both methods simultaneously.

For more information about designing Active Directory support, including prestaging by using scripts, see “Designing the Active Directory Infrastructure” later in this chapter.

Also, when using Startrom.n12 as the startup file, a repetitive installation loop can occur in some situations. This can happen with PXE-enabled client computers that have their BIOS boot configuration set with the network adapter as the first boot device. It can also happen with non-PXE-enabled clients that have their BIOS boot configuration set with the floppy disk drive as the first boot device.

When you use the Startrom.n12 file to automate image installations, it causes client computers that are powering up to immediately initiate a PXE boot, whether from the RIS boot floppy disk or the network adapter — providing that the BIOS boot sequence is set to allow this. When using Startrom.n12, if the boot sequence is set so that computers boot from a PXE-enabled device or the RIS boot floppy disk, every reboot initiates a RIS installation. By contrast, the RIS default startup file Startrom.com provides the client with the option of performing a remote network boot to RIS, which allows the client to avoid the installation loop.

There are two ways to circumvent this problem with automated installations:

- Use the preferred method of altering the BIOS boot configuration of RIS clients so they always boot first from the hard disk and then from the device that boots to RIS.
- Rename the startup files to the default configuration before clients complete the text mode portion of the setup process (after image download), at which time a reboot occurs. For more information about defining new CIW screens and OSC variables see “CIW Design Tasks” later in this chapter.

If you change the boot sequence in the BIOS of RIS client computers so that the hard disk is set as the first boot device, you must also disable the master boot record (MBR) on the boot partition of the hard disk to intentionally cause the first boot attempt to fail. This way, the next boot device in the sequence is the device that boots to RIS over the network, using either the RIS boot floppy disk or a PXE-enabled network adapter. When the text mode portion of the setup process is complete, the disabled disk partition is rebuilt and automatically reactivated to prevent further PXE booting.

To support automated installations on RIS clients, you need to disable the boot partition on each RIS client you want to receive an automated installation. To do this, you can use a tool such as Diskpart.exe, which you can find in the System32 directory of a computer running Windows Server 2003 or Windows XP Professional Service Pack 1. The syntax to run Diskpart.exe is as follows:

```
Diskpart.exe /S:disablepart.txt
```

The file disablepart.txt, which provides input to Diskpart.exe, contains the following commands:

```
SEL DIS 0  
SEL PAR 1  
INACTIVE  
EXIT
```

Diskpart should be run on every active partition on the boot drive of all client computers receiving an automated installation. To simplify administration, you might be able to run this program from a client management system such as SMS.

**Note**

Clients that are configured for an automated installation by using the prestaging script can still have the installation loop problem, if their BIOS boot configuration is not set with the hard disk as first boot device, as described earlier.

## Fully-Automated Installation Design Tasks

When designing a fully automated installation, your primary tasks involve choosing the following:

- The operating system image to configure in the CIW for automated clients.
- The client computers that receive the fully automated installation configuration.
- The configurations for RIS Group Policy options.
- The boot configuration of client computers.

For a job aid to record your design decisions for a fully-automated installation, see “Designing the RIS Deployment Mode and CIW Process” (ACIRIS\_08.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Deployment Mode and CIW Process” on the Web at <http://www.microsoft.com/reskit>).



### Tip

Job aid “Designing the RIS Deployment Mode and CIW Process” (ACIRIS\_08.doc) allows you to record design parameters for either automated or interactive installations. When designing an automated installation, simply skip the sections that apply to interactive installations.

## Defining the Operating System Image

If you want to fully automate the operating system image installation process, it makes sense to provide only one operating system installation option to clients that receive the automated installation. When there is only one operating system image that users are configured to receive, that image is selected automatically and the CIW does not display the operating system choices screen.

For an automated installation, you make a single image available to select users or user groups the same way you make multiple images available for interactive installations: by configuring permissions on answer files and the operating system image folder on your RIS server.

For example, you might have a user group with users that all require an automated installation of a common operating system. For this group, you create an answer file and associate it with a single operating system image. You then set Read permissions on the answer file and image folder to allow each user in the group to receive installation of the operating system.

For this part of your automated installation design process, use the “Operating System Installation Access” section of job aid “Designing the RIS Deployment Mode and CIW Process” (ACIRIS\_08.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Deployment Mode and CIW Process” on the Web at <http://www.microsoft.com/reskit>) to record the operating system image and the user groups that you want to receive it. Also, record the name of the applicable answer file that gives the user group permission to access the operating system image.

You might want to defer recording this information until you design the CIW process. For more information about defining and configuring CIW operating system installation options, see “Interactive Installation Design Tasks” earlier in this chapter.

### **Choosing Clients for Automated Installation**

To provide an automated installation to all clients that contact a RIS server, you can rename the Startrom.n12 file in the \Remoteinstall\OSChooser\i386\ folder on your RIS server to Startrom.com. However, this method does not apply to RIS referral servers since these servers only provide clients with referrals to other RIS servers, which in turn supply the appropriate boot files. For more information about RIS referral servers see “RIS Server Configuration Design Tasks” later in this chapter.

For example, you might have a particular group of clients, configured to be serviced by a single RIS server, for which you want to provide automated installations. In this situation, renaming the Startrom.n12 file to Startrom.com is the best solution.

If you need to configure only certain clients for automated installations, you must explicitly specify which clients receive Startrom.n12 and which clients receive Startrom.com. You can only do this if you prestage clients in Active Directory and specify the startup files for each prestaged computer account as part of the input file to the prestaging script. This way, you can provide an automated installation to any client serviced by any RIS server that is configured to respond to known clients. To find the prestaging script, see the Remote Installation Scripts link on the Web Resources page <http://www.microsoft.com/windows/reskits/webresources>).

For this part of your automated installation design process, use the “Automated Installations” section of job aid “Designing the RIS Deployment Mode and CIW Process” (ACIRIS\_08.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Deployment Mode and CIW Process” on the Web at <http://www.microsoft.com/reskit>) to record the following information:

- The RIS server name.
- The default startup file configuration you intend to use on your RIS server.
- Whether you prestage clients and specify startup files.
- The users or groups you want to receive an automated installation.

## Defining the Group Policy Configuration

When providing automated installations, you want users to be able to start their computers, log on, and initiate the installation process without providing any further input. To assure that this occurs, you can configure the RIS-related Group Policy options so that clients receive an installation based on the **Automatic Setup** option. This means that clients do not have to specify a computer account name and an Active Directory location during the CIW process. This option works well for clients that have prestaged computer accounts in Active Directory and for non-prestaged clients that receive a computer account name and location based on preconfigured RIS server settings.

It does not matter if you prestage by creating computer accounts from the Active Directory extension on your RIS server, or if you prestage by using the prestaging script. In either case, you can configure these clients with the **Automatic Setup** option to support automated installations. However, when prestaging from the Active Directory extension, you are limited to providing automated installations to all clients configured to be serviced by the RIS server, because the extension does not provide any options for specifying the startup file.

The approach that gives you the most flexibility is to prestage clients by using the prestaging script, specify the startup file each client uses, and set the Group Policy option to **Automatic Setup**. You can create as many Group Policy objects as you need to configure the user groups that will receive an automated installation.



### Note

When designing a fully-automated installation, you might want to disable the **Restart Setup** and **Tools** options in Group Policy settings

For example, you might design a fully-automated installation that requires implementing a process such as the following:

- Create a Group Policy object and set the **Automatic Setup** option.
- Apply the Group Policy to a particular user group for which you want automated installations to occur.
- Prestage computer accounts for the users in that group and specify the use of Startrom.n12 file for those users.
- Create an answer file for the group and configure permissions to view a single operating system image.

For this part of your automated installation design process, use the “Group Policy Configuration” section of job aid “Designing the RIS Deployment Mode and CIW Process” (ACIRIS\_08.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Deployment Mode and CIW Process” on the Web at <http://www.microsoft.com/reskit>) to record the Group Policy name, Group Policy configuration, and the user group(s) to which it applies.

You might want to defer recording this information until you design the CIW process. For more information about configuring Group Policy setup options in the CIW, see “CIW Design Tasks” later in this chapter.

### Defining the Boot Configuration

To ensure that your automated installations function as expected, you need to define the proper boot configuration by making the appropriate choices:

**Startup file** Choose which method you intend to use for the startup file configuration:

- Change the names of the startup files on a RIS server to enable all clients serviced by the RIS server to perform a remote network boot of an automated installation.
- Prestage automated installation clients in Active Directory and configure startup files for each client.

You might have already recorded these parameters in job aid “Designing the RIS Deployment Mode and CIW Process” (ACIRIS\_08.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Deployment Mode and CIW Process” on the Web at <http://www.microsoft.com/reskit>) when reviewing the “Choosing Clients for Automated Installation” section, earlier in this chapter. If not, record them now.

**Boot sequence** Choose the client computers on which to configure the appropriate BIOS boot sequence. For automated installations, you must set the boot sequence to use the hard disk as the first boot device and the network adapter (or the floppy disk drive in the case of non-PXE enabled clients) as the second device.

**Hard drive** Choose the client computers for which you must disable all active partitions on the boot drive, using the Microsoft Diskpart.exe tool.

For this part of your automated installation design process, use the “Automated Installations” section of job aid “Designing the RIS Deployment Mode and CIW Process” (ACIRIS\_08.doc) to record the BIOS boot sequence you define for specific clients.



## Designing the CIW Process

After a RIS client computer successfully executes a remote boot to a RIS server, the CIW displays on the client and directs the user to the correct choices for installing an operating system. You can customize the CIW process by configuring which setup and operating system installation options the CIW presents to the user. Also, you can customize CIW screens to support your organization's internal requirements by including items such as Help Desk contact information and other pointers. The CIW supports installations of both Risetup and Riprep operating system images on the client computer in either the interactive or fully-automated mode.

A primary consideration when designing the CIW process is the sophistication level of the users who perform the remote installations, because this influences your choice between deploying interactive and automated installations. In turn, the design of the CIW process is affected by the installation type you choose. If you have not done so already, review "Designing for the RIS Deployment Mode" earlier in this chapter and document the appropriate design decisions using the suggested job aids.

---

### CIW Design Background

The CIW is a text-based tool that guides the user through the remote operating system installation process. The CIW is the first user interface that displays on the client computer after the user installing the operating system begins the remote boot process.

After a RIS client successfully connects to a RIS server for remote installation of an operating system, a startup boot file downloads from the RIS server to the client. In most cases, this is the default startup file Startrom.com. When the default startup file downloads, it prompts the user performing the installation to press the F12 key, at which time the CIW downloads to the client via TFTP. However, the RIS client can also download startrom.n12 or startrom.n12 renamed to startrom.com for an automated installation, if you appropriately configure the RIS client and RIS server. For more information about the remote boot and installation setup processes, see "Process for Deploying RIS" earlier in this chapter.

The CIW displays whether you configure the user to receive an interactive installation (initiated by pressing the F12 key) or an automated installation. However, in fully automated installations, you typically do not provide any setup or other installation options to the user, which minimizes the number of default CIW screens that are presented.



#### Important

You must not remove the Welcome, Logon, or Summary screens from the CIW configuration, and you must have at least one screen that has the `<meta server action=dnreset>` tag.

## CIW Default Configuration

The default configuration of the CIW process provides basic guidance for installing an operating system by using RIS. You can use the default configuration or you can modify it to accommodate your unique requirements. The following is a brief summary of processes that occur in the default CIW configuration.

When the CIW first downloads to the client computer, the Welcome screen displays. After the user responds to the welcome, the CIW displays the Logon screen which prompts the user to log on to the network with credentials that include the user account, password, and logon domain. After Active Directory validates the user's logon credentials, RIS checks certain Group Policy options to verify the installation configuration for the user. The CIW then presents the specific setup options the user is configured to receive.

After the user specifies the appropriate information for setup options, the CIW displays operating system choices, which can include selections for both Risetup and Riprep images. Following selection of an operating system image and display of the Caution and CIW Summary screens, the installation process begins.

## CIW Default Screens and User Interaction

When you install RIS and run Risetup.exe, a default set of CIW screens is installed on your RIS server. These screens guide RIS clients through the part of setup that requires user interaction. Use job aid "The CIW Process" (ACIRIS\_11.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see "The CIW Process" on the Web at <http://www.microsoft.com/reskit>). You can use this information as a reference when considering the details of your CIW design process.

## CIW Screen Functions

The CIW screens that install with your RIS server consist of text files with an .osc extension. These screens consist of a default set of files and several example files that show how to enhance CIW functionality. The examples include files that display a multilanguage Welcome screen and a screen that prompts the user for the administrator password.

The default CIW screens provide the basic functionality you need to perform remote operating system installations on client computers in your organization. You can choose to use the default screens or you can build your own customized screens. This section describes the functionality provided by the CIW screens and various modifications you can make to them.

### Welcome screen

The Welcome screen is a file named Welcome.osc. This screen is the first to display to the user installing the operating system by using RIS. You can modify this screen to include the following:

- Custom information, such as a company-specific message or other preinstallation guidance, which you can add using OSChooser Markup Language (OSCML) tags.
- Custom language options.

For an example of a multilanguage Welcome screen, see the file `Multilng.osc` in the following directory path on your RIS server:

`RemoteInstall\OSChooser\language\`

For more information about defining a multilanguage CIW process, see “CIW Design Tasks” later in this chapter.

### Logon screen

The Logon screen is a file named `Login.osc`. This screen requires the user to log on to the network with valid user credentials consisting of user name, password, and domain name. After the user successfully logs on to the network, RIS uses the user credentials and the Group Policy options applied to the user to determine which setup options the user is configured to receive. If the logon attempt is unsuccessful, the CIW prompts the user to log on again.

You can modify this file to cause a new screen to display that prompts the user to enter the administrator password. For an example of how you can do this, see the file `LoggedIn.osc` in the following directory path on your RIS server:

`RemoteInstall\OSChooser\language\`



### Caution

If you customize `Login.osc`, be careful not to modify any of the values within the following OSML tags:

```
<INPUT NAME="NTLMV2Enabled" VALUE=%NTLMV2Enabled%  
MAXLENGTH=255 type=VARIABLE>
```

```
<INPUT NAME="ServerUTCFileTime" VALUE=%ServerUTCFileTime%  
MAXLENGTH=255 type=VARIABLE>
```

Changing any of these values causes you to lose NTLM v2 support.

### Setup options screen

The Setup Options screen is a file named `Choice.osc`. This screen displays setup options to the user based on the Group Policy configuration applied to the user. You configure Group Policy setup options by accessing the Group Policy Object Editor from the Active Directory extension on your RIS server. Setup options consist of Automatic Setup, Custom Setup, Restart Setup, and Tools. For more information about Group Policy configurations and defining CIW setup options in Group Policy, see “CIW Design Tasks” later in this chapter.

### Error screen

The Error screen is a file named `Dupauto.osc`. This screen displays to the user if RIS finds a duplicate UUID for the client computer in Active Directory. The screen instructs the user to contact the network administrator.

**Operating system choice screen**

The Operating System Choice screen is a file named `Oschoice.osc`. This screen displays a list of operating system images on the RIS server that are available to the logged-on user. If there is only one possible operating system image that the user is configured to install, then that image is selected and the user does not see this screen.

You can add operating system image choices to this screen by setting permissions on the answer files associated with the images you want to add. This causes additional operating system choices to automatically display to the users who have permission to install them, providing that the users are also configured to be serviced by the RIS server that hosts the images.

**Note**

To make operating system images available to RIS clients, you must also configure Read permissions for the image folder on your RIS server.

You can choose to automate the operating system installation choice or you can provide a selection of images to the user.

**Caution screen**

The Caution screen is a file named `Warning.osc`. This screen displays a warning message to users indicating that an operating system will be installed on their computers. The message also indicates that this action causes the hard disk to be repartitioned and formatted and that all existing data will be lost.

**Summary screen**

The Summary screen is a file named `Install.osc`. This screen displays information gathered by the CIW, including the following:

- Computer name
- Computer UUID
- RIS server hosting the installation

By this point in the process, the RIS server has created a computer account object in Active Directory for the client computer. RIS can now readily identify this computer and its associated installation settings, should an operating system need to be reinstalled. The installation now begins if the user presses any key on the keyboard.

**Other error screens**

There are additional screens in the \OSChooser subdirectory on your RIS server that can display when an error occurs. For example, an error might occur if the user enters an incorrect user name or password. When RIS encounters an error, it retrieves the error code (such as 20008 for a login error) and changes it to its hexadecimal equivalent value (00004e28) and appends .osc to the result to derive an error screen file name such as 00004e28.osc. RIS then checks the language directory in use for a screen file with that name. If RIS finds an error screen with a matching name, that screen displays. If RIS cannot find a matching error screen name, an internally generated error message displays. You cannot customize this internally generated error message, however, you can customize the CIW error screens using OSCML tags, just as you can for other CIW screens.

**Custom screens**

You can customize existing screens or create new screens for the CIW using OSCML tags. For new and existing screens, you can use OSC variables to capture user input. For more information about OSC variables, see the discussion about defining new CIW screens and OSC variables later in this section, and see job aid “Reserved OSC Variables” (ACIRIS\_12.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Reserved OSC Variables” on the Web at <http://www.microsoft.com/reskit>). For more information about OSCML tags, see job aid “OSCML and Client Installation Wizard Variables” (ACIRIS\_13.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “OSCML and Client Installation Wizard Variables” on the Web at <http://www.microsoft.com/reskit>).

---

**CIW Design Tasks**

When designing the CIW process, your primary tasks are to choose the following

- The operating system installation options you want to present to clients.
- The setup options you want to provide to clients.
- The CIW configuration you want to provide.

For a job aid to record your design decisions for your CIW process, see “Designing the RIS Deployment Mode and CIW Process” (ACIRIS\_08.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Deployment Mode and CIW Process” on the Web at <http://www.microsoft.com/reskit>).

## Defining CIW Operating System Installation Options

The operating system installation options that you provide in the CIW enable users to receive the correct operating systems on their computers. By setting explicit user or group security permissions on the answer file associated with specific operating system images on your RIS server, you can control which installation images the CIW displays to users or user groups. You can restrict users and user groups to viewing a single image in the CIW or you can make all operating system images on your RIS server available to them.

Each Risetup or Riprep image that you add to your RIS server has an associated \Templates directory that contains a default answer file (Ristndrd.sif or Riprep.sif) and any additional answer files that you create and associate with that image. These are the answer files on which you configure permissions to cause the CIW to display operating system image installation options on the OSChoice screen. However, you must set these permissions from your RIS server **Properties** dialog box, rather than setting them directly on the answer files in the \Templates directory.

Because selecting individual users for specific image access is time consuming, consider using security groups when applying permissions on answer files. This way, any new users that you add to a particular group automatically receive the correct operating system image installation options.



### Caution

The default security permissions allow the **Everyone** group access to operating system images displayed in the CIW. To restrict access to operating system images, remove the **Everyone** group, and add only the users that you want to access the images.

For this part of your CIW design process, it is unnecessary to record your operating system installation access configuration options if you specified them earlier in “Defining the Operating System Image” using job aid “Designing the RIS Deployment Mode and CIW Process” (ACIRIS\_08.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Deployment Mode and CIW Process” on the Web at <http://www.microsoft.com/reskit>). However, if you did not do so, decide on them now and record them under the “Operating System Installation Access” section in the job aid.

## Defining CIW Setup Options in Group Policy

The setup options that you configure in Group Policy help guide users to the correct choices for installing their operating systems. When determining the setup options you want to provide to users, you need to consider the sophistication level of the users who will be installing using RIS. You can provide advanced users with options that allow them to:

- Specify a name for their computer accounts and a location in Active Directory, if you enable the **Custom Setup** option.
- Restart a failed installation attempt, if you enable the **Restart Setup** option.
- Access maintenance and troubleshooting tools, if you enable the **Tools** option.

For less knowledgeable users, you might want to prestage client computers in Active Directory, automate installations for those computers, and enable the **Automatic Setup** option in the Group Policy object that users at the client computer receive. If the Group Policy object applied to the users is configured with the **Automatic Setup** option, then the CIW does not present computer account setup options to the users. In this case, the CIW only displays the following installation options:

- Those that offer a choice of operating systems the user can install.
- Those that exist on any other custom screens you create.



### Tip

You can configure the CIW to not present any setup or operating system installation options if you configure a fully-automated installation. You can also configure both **Automatic** and **Custom Setup** options to simultaneously provide for less knowledgeable users and also allow advanced users to enter their own input.

You can apply a setup option configuration for clients by using the default domain Group Policy settings, or you can create new Group Policy objects that you customize and apply to specific user security groups. If you apply a new Group Policy object that has any of the setup options set to “Not Configured”, the settings for the corresponding options in the default domain policy apply.

For this part of your CIW design process, it is unnecessary to record your Group Policy configuration options if you specified them earlier in “Designing for the RIS Deployment Mode” using job aid “Designing the RIS Deployment Mode and CIW Process” (ACIRIS\_08.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Deployment Mode and CIW Process” on the Web at <http://www.microsoft.com/reskit>). However, if you did not do so, record your Group Policy setup option design choices after evaluating the information in the following paragraphs.

**Automatic setup**

This option provides the simplest way to install an operating system on the client computer. When the Group Policy object applied to the client is configured with this option, RIS searches Active Directory for a computer account object with a UUID that matches the UUID of the client computer. If RIS finds a match, the client computer is named according to the prestaged computer account name. If RIS does not find a match, the client computer account is named and located according to the automatic naming format and Active Directory location that you preconfigured on the RIS server.

**Custom setup**

This option allows users to override the automatic computer naming process and the default location specification in Active Directory for client computer account objects. However, if the user leaves either the computer name or location field blank, RIS uses the automatic naming and location process.

The **Custom Setup** option is similar to the **Automatic Setup** option, although you can use **Custom Setup** to set up the client computer for other users. Because the default configuration of a RIS-based installation is to automatically create computer account names based on the user who logs on to the client computer, it is impractical to use the **Automatic Setup** option when you need to set up another user's computer. For example, Help Desk personnel can use the **Custom Setup** option to preinstall an operating system on a client computer, prior to delivery to the client.

If the name and location the user enters under the **Custom Setup** option and the client UUID match the name, location, and UUID of an existing computer account object, the existing computer account object is reused. If only one of the fields between name, location, and UUID match, a duplicate name or duplicate UUID error screen displays. However, because the user can bypass the error screen, do not use the **Custom Setup** option for prestaged client computers in installations that users perform directly.

**Restart setup**

This option allows users to restart a failed installation attempt, which might occur if the installation process fails or network connectivity is disrupted during the text-mode stage of the setup process. This part of setup is where the CIW process runs prior to the image copy stage. If you provide this option, a **Restart Setup** command is available to users the next time they restart their computers. If the user executes the command, the operating system installation process restarts using the information provided in the previous installation attempt. Display of this command is controlled by the client-specific temporary answer file that RIS generates and then deletes before running Mini-Setup.

**Tools**

This option allows users to access maintenance and troubleshooting tools for use prior to completing the operating system installation. Such tools include a system flash BIOS update tool, diagnostic tools, or other tools provided by third parties.



## Defining the CIW Configuration

You can choose to use the default CIW configuration or create a custom configuration. If the default CIW configuration is adequate for your purposes, you can use it as a quick way to provide basic installation guidance to your clients. If necessary, review the functionalities described in “CIW Screen Functions” earlier in this chapter before making your decision.

For a customized configuration, you can build new screens by renaming existing screens and modifying them with OSCML tags. You can also modify existing screens by adding certain OSCML tags that allow you to provide additional information. In addition, you can construct screen prompts for custom user input and use OSC variables in your answer files to capture the input information. You can also use one of the sample .osc files as a new CIW screen to display to users.

If you anticipate network problems, you can even create waiting screens to allow you to debug network delays that might exist between clients and the RIS server, or between the RIS server and the domain controller. For more information, see the discussion about defining new CIW screens and OSC variables later in this section.



### Note

To modify CIW screens (.osc files), you can use a text editor such as the Notepad application.

For this part of your CIW design process, decide if you want to use the default CIW configuration. If you think you will need custom screens or modifications to existing screens, choose a custom CIW configuration. To record your decision, use the “CIW Configuration” section in job aid “Designing the RIS Deployment Mode and CIW Process” (ACIRIS\_08.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Deployment Mode and CIW Process” on the Web at <http://www.microsoft.com/reskit>).

If you choose the default configuration, you can skip the remainder of this section. If you choose to define a custom CIW configuration, you need to decide if you want to do one or more of the following:

- Add new screens to the CIW process, including wait screens.
- Modify existing screens with custom prompts or information displays.
- Remove any screens from the CIW process.

**Defining new CIW screens and OSC variables**

You can customize the CIW process by creating additional screens that require the user to provide custom information to complete the installation. This can assist you when creating interactive deployments because it gives you some flexibility in the way you gather user input.

For example, you can build a new screen from an existing screen by modifying its contents using OSCML tags. You can then add user input prompts to the new CIW screen. You also use an OSCML tag to define which screen the CIW displays next, so you can insert a new screen into the CIW process at the correct point. This tag has the following format:

```
<FORM ACTION = "SCREENNAME">
```

When you add input prompts, you must also have a method to capture the user input information. To do this, you create OSC variables in the image answer file. When the CIW runs, RIS replaces the OSC variables in the answer file with the values the user enters in the CIW screen input prompt. RIS then uses these values in the temporary answer file it creates for the client installation configuration.

You can create an OSC variable for any answer file value that works with an unattended setup process in addition to those specifically designed for RIS. However, you must specify OSC variables in your answer file by enclosing them in percent signs so RIS can identify and parse them correctly. For example, you could create prompts on a custom CIW screen that ask users to specify the X and Y resolution and the refresh rate for their video display. To do this, you must include the following OSCML tags in the new screen and specify input name strings such as the following:

```
<INPUT NAME="X-res">
```

```
<INPUT NAME="Y-res">
```

```
<INPUT NAME="Refresh">
```

Then, in your answer file, you need to specify the OSC variables that capture the user input. You can do this by setting the appropriate unattend values equal to the corresponding OSC variables in the unattended [Display] section, as follows:

```
[Display]
```

```
XResolution=%X-res%
```

```
YResolution=%Y-res%
```

```
VRefresh=%Refresh%
```

You can use up to 64 unique OSC variables per client session; however, there are certain variables that are reserved for RIS use only. For a list of these variables, see job aid “Reserved OSC Variables” (ACIRIS\_12.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Reserved OSC Variables” on the Web at <http://www.microsoft.com/reskit>). Also, you cannot define OSC variables prior to the time the user logs on to the network, with exception of the %language% variable, which the user can only set before logging on. This allows users to select the proper language in which to proceed in the installation. For more information about OSCML tags, see job aid “OSCML and Client Installation Wizard Variables” (ACIRIS\_13.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “OSCML and Client Installation Wizard Variables” on the Web at <http://www.microsoft.com/reskit>).

The logon process from a PXE client to a Windows Server 2003 RIS server uses NTLM v2 by default to encrypt the user name and password sent between the client and RIS server. After authentication, the client and server communicate using SMB. For more information about NTLM v2, see “Evaluating the NTLM Authentication Level” earlier in this chapter.

From this point forward in the CIW process, you can create any OSC variables you need for custom or existing screens, as long as you associate them with sections in the Unattend.txt answer file. For more information about sections in the Unattend.txt answer file, see “Unattended.txt” in the *Microsoft® Windows Server 2003 Corporate Deployment Tools User’s Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.

Also, if you observe significant time delays between CIW screens, you might consider inserting waiting screens at the appropriate point of the CIW process. One way you might observe where delays are occurring is to configure waiting screens in a test CIW configuration and perform a test installation in your production network environment. If there are no delays, the waiting screens display only for a moment and then the next CIW screen appears. Otherwise, the waiting screens display for the length of the network delay. Once you know where the delays are occurring, you can include waiting screens in your user CIW process.

For example, users might experience a delay between the time they log on and the time they receive the operating system choice screen Choice.osc. To improve the user experience, you can place a waiting screen between Login.osc and Choice.osc with a statement that asks the user to please wait while their logon credentials are verified. Also, slow network access to the domain controller might occur when creating computer account objects in Active Directory. To accommodate the delay, you might add a waiting screen between Choice.osc and Autodup.osc asking the user to wait while creating their computer account.

Lastly, when you insert a new or modified screen into the CIW process on a RIS server, you enable all users who are configured to use the RIS server to view the new screen. Also, you must include changes to the CIW process on each RIS server because there is no capability to synchronize changes to .osc files across multiple RIS servers.

**Note**

You might want to test your CIW process in your RIS test environment before making changes to the CIW process on RIS servers in your production environment

For this part of your CIW design process, use the “CIW Configuration” section in job aid “Designing the RIS Deployment Mode and CIW Process” (ACIRIS\_08.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Deployment Mode and CIW Process” on the Web at <http://www.microsoft.com/reskit>) to record the following information:

- New screens to be added, including wait screens.
- Insertion points in the CIW process for new screens.
- New user input prompts.
- OSC variables to create for new user prompts and the associated answer file entries.

Also, use the “Operating System Installation Access” section of job aid “Designing the RIS Deployment Mode and CIW Process” (ACIRIS\_08.doc) to indicate which answer files require configuration with OSC variables.

**Defining modifications to existing CIW screens**

You can modify existing screens with the same techniques that you use for customizing new CIW screens. This means you use a combination of OSCML tags in your .osc files and OSC variables in your image answer file (in cases where you are gathering custom user input). However, remember that you cannot create OSC variables in screens that display before the Logon screen, with exception of the %language% variable, which you can use in the Welcome screen configuration.

When you need to provide custom information in a CIW screen, you can use the following OSCML tag to add the text:

```
<BODY>
```

```
Text you want to provide.
```

```
</BODY>
```

For this part of your CIW design process, use the “CIW Configuration” section in job aid “Designing the RIS Deployment Mode and CIW Process” (ACIRIS\_08.doc) to record the following information:

- Names of the existing screens you want to modify.
- Input prompts or information you want to provide.
- OSC variables and answer file entries you want to use.

Also indicate the answer files that require configuring with OSC variables. Use the “Operating System Installation Access” section of job aid “Designing the RIS Deployment Mode and CIW Process” (ACIRIS\_08.doc) to record this information.

### **Defining screens to remove**

There might be specific screens you want to remove from the CIW process. This could include the Setup Options, Error, Operating System Choice, and Caution screens. You might want to do this for RIS clients that receive an automated installation, or if you decide you don’t want a particular screen to display. However, be aware that you must not remove the Welcome, Logon, or Summary screens.

If you want to remove a screen from the CIW process, you can change the target of the appropriate OSCML tag so that it no longer calls the screen. These OSCML tags exist in each CIW screen and they point to the next .osc file the CIW displays. For example, the following OSCML tag in the Oschoice.osc file calls the Warning.osc screen:

```
<FORM ACTION = "WARNING">
```

Therefore, if you want to skip the Warning screen, you can change the target screen of this tag to the Summary screen.

For this part of your CIW design process, use the “CIW Configuration” section of job aid “Designing the RIS Deployment Mode and CIW Process” (ACIRIS\_08.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Deployment Mode and CIW Process” on the Web at <http://www.microsoft.com/reskit>) to identify the screens you want to remove from the CIW process.

At this point, you should have gathered enough information to identify the new CIW screen sequence. Record this information in job aid “Designing the RIS Deployment Mode and CIW Process” (ACIRIS\_08.doc) under the “New CIW Sequence” section along with the RIS servers to which you want the new configuration to apply. Also, if you want to test the new CIW configuration in your RIS test environment, select the appropriate check box in the “New CIW Sequence” section.

**Defining a multilanguage CIW process**

If you need to support multiple languages, you can use a single RIS server to provide service to clients that install different language versions of the Windows Server 2003 or Windows XP Professional operating systems. You can modify the Welcome screen to include the language options you want the RIS server to support. You can find the Welcome.osc file in the \OSChooser directory on your RIS server. Also in this directory is the sample Multilng.osc file that shows how to configure multilanguage support.

The CIW screens that display following the Welcome screen are obtained by RIS from the specific language folder in the \OSChooser directory. The list of operating system images presented to the user is restricted to images for the language selected. For each language version you want to make available to users, you must provide a set of CIW screens in a separate language folder in the \OSChooser directory. The \OSChooser\English version is provided by default.

Certain language restrictions apply to the CIW; these include not providing support for the following:

- Non-101 key keyboards.
- Non OEM fonts.
- Multi-Byte Character Set (MBCS)/Unicode character sets.

These restrictions apply to data used within the CIW, including computer, domain, and directory or file names such as answer file names. It also applies to any example or descriptive text you display to users and to the text that users input to the CIW, such as user names, passwords, and domain names. Because of these restrictions, you must ensure these user input strings do not contain any non-ASCII characters, since they cannot be used within the CIW. Furthermore, even though you can use a different set of CIW screen files for each language you want to make available, in many cases it is not possible to create screens that are fully localized to a specific language using available character sets.

Also, to support Riprep images in different languages, a Risetup (CD-type) image of the language must also exist on your RIS server. This is necessary to supply files such as device drivers that are needed during installation of the Riprep image, but that did not exist on the master installation from which you derived the Riprep image.

For this part of your CIW design process, record your decision to provide a multilanguage CIW process under “CIW Configuration” in job aid “Designing the RIS Deployment Mode and CIW Process” (ACIRIS\_08.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Deployment Mode and CIW Process” on the Web at <http://www.microsoft.com/reskit>). Also indicate your choices for the language options you want to provide using the “Required User Input” section of job aid “Designing the RIS Deployment Mode and CIW Process” (ACIRIS\_08.doc), if you did not do so in “Defining User Input” earlier in this chapter.

## Designing the RIS Server Configuration

You can design your RIS server configuration to accommodate smaller localized networks as well as full scale corporate networks. In smaller networks of 100 or less client computers, you can minimize the number of RIS servers you need to service client requests for operating system installations. However, in larger network environments, you need to carefully consider the following:

- Where to place RIS servers on the network so as to minimize the impact of RIS traffic.
- Where RIS clients are located in proximity to the RIS servers that service them.
- How many clients you intend to service.
- How you distribute different operating system images to various user groups.
- What security methods you apply to ensure secure operating system installations.
- How you configure your Active Directory infrastructure to support RIS.

To accommodate full-scale corporate environments, you will need multiple RIS servers across your network, preferably using a combination of referral servers that accept, process, and forward client requests, and install servers, which provide the client with boot files, CIW screens, and the actual image download.

---

### RIS Server Configuration Design Background

The way you design your RIS server configuration directly impacts its performance. For example, where you place your RIS servers on the network makes a difference because RIS servers generate heavy traffic during periods when clients are installing operating system images. Also, the number of RIS servers you have plays a role in installation performance because there is a limit to how many clients each RIS server can handle before time-outs occur during client service requests. In addition, by making use of multiple distribution points to provide different operating system images to RIS clients, you can mitigate network traffic and provide faster installation times to clients.

Another factor that impacts your RIS server configuration is the way you implement RIS server security. In corporate environments, you need to design a RIS server configuration that provides secure responses to clients requesting service. To do this, you need to set specific RIS server properties, provide security for non-prestaged clients, and secure the operating system images that you distribute to clients. You can also include prestaging RIS client computer accounts in Active Directory as part of your design, to maximize the security of RIS-based operating system installations.

## RIS Server Configuration Design Tasks

When designing your RIS server configuration, your primary tasks are to define the following:

- Network deployment configuration and the supporting Active Directory infrastructure
- RIS server properties and other RIS configuration parameters.
- RIS security configuration.

For a job aid to record your design decisions for your RIS server configuration, see “Designing the RIS Server Configuration” (ACIRIS\_09.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Server Configuration” on the Web at <http://www.microsoft.com/reskit>).



### Note

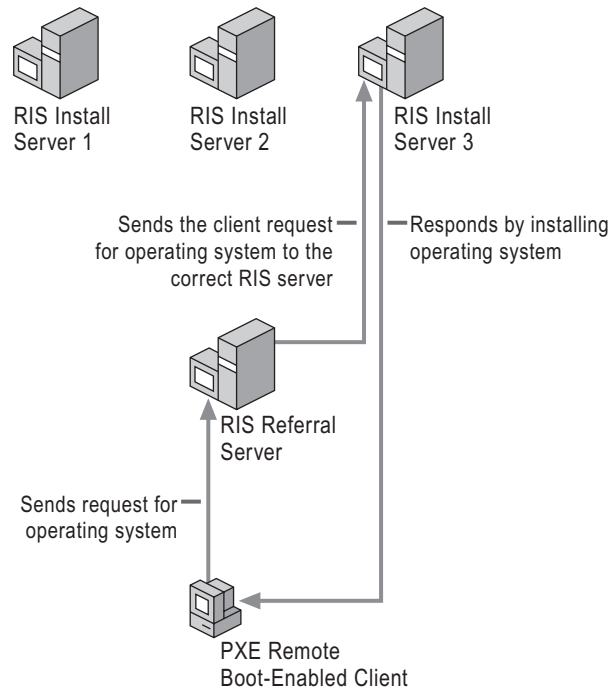
Although your Group Policy settings are part of your RIS server configuration, it is unnecessary to design them here because you should have already made those design decisions in “Designing for the RIS Deployment Mode” earlier in this chapter, and recorded them in job aid “Designing for the RIS Deployment Mode”(ACIRIS\_08.doc).

## Designing the RIS Network Deployment Configuration

RIS servers are dependent on your network configuration: the way you deploy and manage your RIS servers on the network determines how they perform. Depending on how you place and configure your RIS servers, one operating system image can support multiple Active Directory sites, domains, and organizational units, or you can provide multiple customized images that you distribute to clients from strategically placed RIS servers.

Because each RIS server can only handle a limited number of simultaneous client installations, you might consider load balancing client service requests by using a RIS referral server. Figure 4.6 shows a basic RIS configuration unit that illustrates the relationship between PXE-enabled remote boot clients, a RIS referral server, and RIS install servers on the network that provide service to clients.



**Figure 4.6 RIS Server Network Deployment**

In Figure 4.6, a PXE-enabled remote boot client requests the remote installation of an operating system. The request is passed to the RIS referral server, which is configured with the **Do not respond to unknown clients** option. This allows only prestaged clients to be acknowledged by the RIS referral server. The RIS referral server checks Active Directory to verify whether the client has a prestaged computer account and if it is configured to receive service from a specific RIS install server. If it finds a prestaged computer account and a designated RIS install server, the RIS referral server passes the request to the appropriate RIS install server (RIS Install Server 3) in Figure 4.6. The client then downloads the CIW and begins the installation process.

RIS Install Servers 1, 2, and 3 are install servers that only provide operating system installations and do not respond to initial client requests for service. Conversely, the referral server does not provide image support, but does answer initial client service requests.

Figure 4.6 shows how RIS referral and install server configurations can work in an enterprise setting. In this configuration, you can apply tight control to which clients can access which RIS servers. This enables you to load-balance client service requests to ensure that each RIS server is not overloaded. You have this capability because you can specify which RIS server services which clients when you prestage client computer accounts in Active Directory. When you do this, be sure not to configure more than 75 clients per RIS server if you expect heavy service request traffic from clients. Alternatively, you can implement a simpler solution by configuring all RIS servers to respond and provide service to all RIS clients, however, this foregoes the additional security gained by using prestaged RIS clients.

To design a RIS server network deployment that includes configuration units such as the one depicted in Figure 4.6, begin by deciding the following:

- The number of RIS servers you require (including both RIS image and RIS referral servers).
- Where you will place RIS servers.
- How you will distribute RIS server images to clients.

### **Defining the number of RIS servers**

The number of RIS servers you need is largely dependent upon how many RIS clients you need to support. You might need multiple RIS servers to support the clients in a large organization or only one RIS server if you are deploying Windows XP Professional on a small LAN or network segment.

The number of RIS servers you will need is impacted by the demand for new, upgrade, or custom operating system installations. As a result, you will need to determine your needs prior to deploying a standard desktop configuration of Windows XP Professional or other operating systems to your clients. Once you determine your needs, you can calculate how many RIS servers to deploy. You can base your estimate on the following metric for best case scenarios: one RIS server can send multiple operating system images over the network for up to 75 clients simultaneously.

The speed of your network and the hardware you use on your RIS server to support image distribution can also have a bearing on how many RIS servers you need. If you have slower network connections or RIS server hardware with marginal capabilities, you will need more RIS servers to handle client service requests to avoid network traffic bottlenecks during periods when RIS servers are active. If you follow the hardware recommendations specified in “Evaluating RIS Server Hardware Requirements” earlier in this chapter, you will be able to maintain support for the maximum number of clients per RIS server.

For load balancing and security reasons, consider using prestaged clients with a RIS referral and install server configuration. If you decide in favor of this configuration, then you must also determine the number of RIS referral servers you need to use. A RIS install server should be in close proximity to the clients it services, but a RIS referral server can pass client service requests to RIS install servers that are located across routers and domains. This is possible as long as the routers are enabled to pass DHCP traffic and there is a trust relationship between domains. As a general guideline for calculating how many RIS referral servers you will need, you can use a metric of one RIS referral server for every three RIS install servers.

For this part of your RIS server configuration design process, use the “RIS Network Deployment Configuration” section in job aid “Designing the RIS Server Configuration” (ACIRIS\_09.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Server Configuration” on the Web at <http://www.microsoft.com/reskit>) to record the total number of clients you need to support and the total number of RIS servers you need to provide image services. Also include the total number of RIS referral servers that you will need.

### Defining RIS server placement

The primary issues concerning RIS server placement involve where you physically locate the server and where you place it in your Active Directory infrastructure. For more information about designing your Active Directory infrastructure, see “Designing the Active Directory Infrastructure” later in this chapter.

As a general guideline, place RIS servers in close physical proximity to the client computers they service rather than making connections across a WAN link. However, it might be necessary for your clients to locate a RIS server across a router or domain. When this is the case, the router must be configured to pass DHCP packet traffic and there must also be a trust relationship between domains. When considering RIS server placement in your network, you might also consult your DHCP scopes to analyze your domain structure.

In large organizations, do not place your RIS server on a DHCP server. This avoids potential failures in DHCP service if the RIS server becomes overloaded with client service requests. For more information about RIS server placement on the network, see “Assessing RIS Server Placement” earlier in this chapter.

Other placement issues are associated with the type of network connection you use to integrate RIS servers into your environment. Slow connections to RIS servers can hinder the speed of your entire network during periods when RIS is active. Inappropriate RIS server hardware that cannot support network demands can do the same thing. As a practical example, if your organization has branch offices, it is best to place a RIS server in each branch rather than attempting to have clients connect to a RIS server across a slow WAN connection.

For this part of your RIS server configuration design process, use the “RIS Network Deployment Configuration” section of job aid “Designing the RIS Server Configuration” (ACIRIS\_09.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Server Configuration” on the Web at <http://www.microsoft.com/reskit>) to record the following:

- The network location or site name.
- The names of RIS install servers that provide service to specific clients.
- Whether you need to enable DHCP on routers for cross-domain client service requests.
- Whether you need to establish cross domain trusts.
- The names of your RIS referral servers and the Active Directory domains/subnets which they support.

**Defining the distribution of RIS server images**

Depending on the size of your network and the number of clients you have, you might need to create a scheme for managing the distribution of multiple operating system images from different RIS servers to ensure quick installations across the network. You can do this by using multiple RIS servers that provide custom operating systems installations to specific clients. To provide specific operating system images to clients from designated RIS servers, you will need to do the following:

- Create the operating system images you want on each RIS server using Risetup.exe or Riprep.exe.
- Create unique answer files and associate them with specific operating system images on each RIS server.
- Set security permissions on the answer files to configure which users or user groups can access the images.

You can also create unique versions of the CIW process with custom .osc files on each RIS server to manage how you identify and distribute images associated with each RIS server. By distributing operating system images from different RIS servers in this manner, you can mitigate network traffic and accelerate the installation process for designated RIS clients.

For this part of your RIS server configuration design process, use the “RIS Network Deployment Configuration” section of job aid “Designing the RIS Server Configuration” (ACIRIS\_09.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Server Configuration” on the Web at <http://www.microsoft.com/reskit>) to record whether you intend to use multiple RIS servers to handle the distribution of a single operating system or multiple operating systems. If you choose multiple operating systems, record the operating system image names, the RIS servers that will host them, and whether you want to use a corresponding custom CIW process on each RIS server.

For more information about creating operating system images, see “Designing for the RIS Installation Type” earlier in this chapter. For more information about customizing the CIW process see “CIW Design Tasks” earlier in this chapter.

## Designing RIS Server Properties

How you configure your RIS server properties has an impact on RIS server performance and function. The properties you can set on a RIS server are located in the RIS server **Properties** dialog box. You can access this dialog box by using the Active Directory extension on your RIS server. To open the dialog box, right-click the RIS server computer account object in Active Directory and select **Properties** to access the **Remote Install** tab. From here you have access to RIS server properties, which includes the following options:

- **Client support.** Consists of options that allow you to determine which clients the RIS server responds to.
- **Computer naming format.** Consists of various options that determine how computer account objects will be named.
- **Computer account location.** Consists of options that determine where the computer account objects will be placed in Active Directory.

To determine the most appropriate settings to use for RIS server properties in your organization, use Table 4.4 as a guide.

**Table 4.4 RIS Server Property Settings**

Use This Setting	When
<b>Client support options</b>	You need to configure the way RIS servers respond to clients requesting installation service. For more information about client support options, see the discussion about designing RIS server security in “RIS Server Configuration Design Tasks” later in this chapter.
<b>Respond to client computers requesting service</b>	You want a RIS server to acknowledge all clients requesting service, including prestaged and non-prestaged clients, to whom the server makes its operating system images available. Use when maximum security is unnecessary or when you are setting up a RIS referral server.
<b>Do not respond to unknown client computers</b>	You want a RIS server to acknowledge only clients with prestaged computer accounts in Active Directory, to whom the server makes its operating system images available. Use when you want to maximize the security applied to RIS clients so unauthorized clients cannot receive an operating system installation.

*(continued)*

**Table 4.4 RIS Server Property Settings (continued)**

Use This Setting	When
<b>Client computer naming format options</b>	You configure the Automatic Setup option in Group Policy, so you can apply the computer naming format to non-prestaged clients and to Custom Setup clients that do not provide input for computer name and Active Directory location.
<b>User name</b>	You want to name the client computer requesting RIS service based on the user name of the operating system installer. This is the default setting.
<b>NP plus MAC address</b>	You want to name the client computer requesting RIS service based on the media access control (MAC) address of the client network adapter.
<b>Custom naming scheme</b>	You want to name the client computer requesting RIS service based on a custom naming format that you specify.
<b>Other name variations</b>	You want to name the client computer requesting RIS service based on name variations such as first name, last name, initial, and so on.
<b>Client account location options:</b>	You want to define the default Active Directory container for all client computer accounts prior to installation.
<b>Default directory service location</b>	You want to specify that the client computer account object is created in the Computers container by default when the client joins the domain. Use when you want the client computer to become a member of the same domain as the RIS server handling the client installation process.
<b>Same location as that of the user setting up the client computer</b>	You want to specify that the client computer account object is created within the same Active Directory container as the user account of the user setting up the computer, for example, in the Users container.
<b>The following directory service location</b>	You want to predetermine where client computer account objects are created in Active Directory. Use when you want to configure an account location for all client computers installed from a RIS server.

**Tip**

If a prestaged client exists in a forest separate from the RIS forest and RIS is configured to not respond to unknown clients, this client will not be answered by RIS. You can fix this by configuring RIS to answer unknown clients and specifying the directory service location in the correct forest where computer accounts are created. Do this using the New Clients tab of the Remote Install dialog box on the RIS server.

For this part of your RIS server configuration design process, use the “RIS Server Properties” section of job aid “Designing the RIS Server Configuration” (ACIRIS\_09.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Server Configuration” on the Web at <http://www.microsoft.com/reskit>) to record the configuration settings you choose from Table 4.4.

### Defining Other RIS Server Configuration Parameters

The **Remote Install** tab also provides you with access to other dialog boxes that allow you to do the following:

- Associate new answer files with existing images.
- Set security permissions on answer files.
- Add new Risetup images to the RIS server.
- Remove tools or view properties of tools provided by third parties.
- Set security permissions on the RIS server computer account object in Active Directory.

From the **Remote Install** tab, you can also browse Active Directory to do such things as display the UUIDs of all your RIS clients along with the RIS servers designated to service them.

#### Defining answer file associations

By clicking the **Advanced Settings** button in RIS server **Properties**, you can define answer file associations on your RIS server. For example, from the **Images** tab, you can associate answer files with existing operating system images. This allows you to provide custom operating system installations based on answer files that you create and tailor for specific user needs. After you associate the answer file with an image, you can set permissions on the answer file to enable specific users to access the image associated with it.



#### Note

In **Advanced Settings** in RIS server **Properties**, setting permissions on an item under **Descriptions** on the **Images** tab sets permissions on answer files associated with images rather than on the images themselves.

You should already have recorded the design decisions that specify which answer files you associate with RIS installation images and the user groups that you permit or deny access to these files. These tasks are part of designing the RIS deployment mode and the CIW process.

**Choosing additional Risetup images to host on RIS servers**

From the **Image** tab of RIS server **Properties**, you can add new Risetup images to your RIS server based on an operating system CD that you provide. If you click the **Add** button on the **Images** tab, a dialog box displays with an option that starts the Risetup Wizard. The design decisions about which Risetup images you intend to host on your RIS server(s), made in “Risetup Image Design Tasks” earlier in this chapter, were recorded using job aid “Defining Risetup Images” (ACIRIS\_07.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Defining Risetup Images” on the Web at <http://www.microsoft.com/reskit>).

**Choosing to remove tools**

From the **Tools** tab, you can remove tools or view the properties of system maintenance and troubleshooting tools provided by third parties. You cannot add tools to your RIS server from the **Tools** dialog box. Only independent software vendors (ISVs) or original equipment manufacturers (OEMs) can provide system maintenance and troubleshooting tools to administrators, technical support staff, and users of client computers. ISVs and OEMs use a custom setup program to add their tools to the `\RemoteInstall` directory on a RIS server.

Your RIS server configuration design might involve removing certain tools from your RIS server so that they are not available to clients. However, note that you can achieve the same objective by using Group Policy settings for specific user groups rather than by deleting the tool entirely. You cannot retrieve a tool once you delete it, except by the OEM reinstalling it. Record which tools you want to delete in the “Other RIS Server Configuration Parameters” section of job aid “Designing the RIS Server Configuration” (ACIRIS\_09.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Server Configuration” on the Web at <http://www.microsoft.com/reskit>).

**Choosing to delegate RIS administrative tasks**

If you decide to delegate administration of your RIS server, you can set permissions on your RIS server computer account in Active Directory from the **Security** tab of RIS server **Properties**. The decision to delegate RIS administrative tasks is addressed in the discussion about assessing delegation of RIS administrative tasks in “Planning Security for RIS Administrative Tasks” earlier in this chapter. If you did record your decision in job aid “Planning RIS Server Security” (ACIRIS\_05.doc) earlier, record the information now in the “RIS Administrative Task Security” section of the job aid. See “Planning RIS Server Security” (ACIRIS\_05.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning RIS Server Security” on the Web at <http://www.microsoft.com/reskit>).



## Designing RIS Server Security

Most RIS server security issues are addressed in “Planning RIS Server Security” (ACIRIS\_05.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning RIS Server Security” on the Web at <http://www.microsoft.com/reskit>). The security design issue details that must now be completed include choosing how to do the following:

- Provide secure responses from your RIS server to clients, with load balancing.
- Provide security for non-prestaged RIS clients.
- Optimize network security for RIS services.
- Provide authorization for your RIS servers.

### Designing secure RIS server responses and load balancing

To control how a RIS server responds to remote boot-enabled clients that request service, set **Client support** options on the RIS server **Properties** dialog box. Available settings consist of the following:

- **Respond to client computers requesting service.** The RIS server responds to all clients requesting service. This is the least secure setting because the RIS server does not distinguish between authorized and unauthorized clients.
- **Do not respond to unknown client computers.** The RIS server only responds to clients that have a prestaged computer account object in Active Directory. This is the most secure setting for your network because it enables you to limit access to only authorized clients that are prestaged in Active Directory.

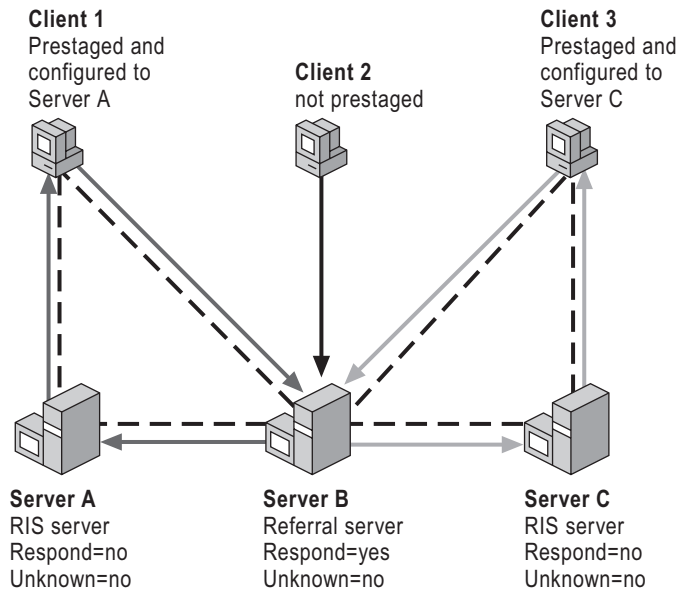
If you configure a RIS server with the **Respond to all clients requesting service** option, you designate that server to handle all client requests for RIS services. In this configuration, you have less security with respect to unknown and possibly unauthorized clients accessing the RIS server. However, you can enhance security by configuring the RIS server to only respond to prestaged clients using the **Do not respond to unknown client computers** option.

In addition, if you prestage all computer accounts and use the RIS referral and install server configuration described in “Designing the RIS Network Deployment Configuration,” you can provide load balancing for client service requests by:

- Dedicating RIS servers as referral servers that acknowledge all initial prestaged client service requests and then provide referrals to the appropriate RIS install servers.
- Using specific RIS install servers to handle service requests from designated clients.

Figure 4.7 illustrates how a referral server responds to non-prestaged and prestaged RIS clients.

**Figure 4.7 Securing Client Request Responses and Achieving Load Balancing With RIS Servers**



**Server Configuration Key:**

Respond- Respond to Client Computers

Unknown- Respond to Unknown Client Computers

In Figure 4.7, only Server B is configured as a referral server because it is the only one that can respond to initial client requests for RIS services. It is also configured to only respond to prestaged or “known” clients. Because Client 1 and Client 3 are prestaged and configured to obtain service from a specific RIS server, they receive replies from Server B that refer them to either Server A or Server C.

In Figure 4.7, Servers A and C cannot reply to initial client service requests, but only provide operating system installation services to Client 1 and Client 3 through referrals from Server B. Client 2 is not recognized by Server B because it is not prestaged and therefore cannot receive service from any RIS server.

If you configure Server B to not use the **Do not respond to unknown client computers** option, then Server B itself replies to service requests from Client 2 and offers itself as the remote boot server. Server B functions this way because it is configured to respond to all clients requesting service (Respond = Yes in Figure 4.7).

If you have not already done so, use the “RIS Server Properties” and “RIS Network Deployment Configuration” sections of job aid “Designing the RIS Server Configuration” (ACIRIS\_09.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Server Configuration” on the Web at <http://www.microsoft.com/reskit>) to record the **Client support** options you choose and whether you want to use the RIS referral and install server configuration.

### **Designing security for non-prestaged RIS clients**

To improve the security of non-prestaged RIS clients, you can control which valid users can create computer accounts in Active Directory during installation. You do this by using the Active Directory **Delegation** feature to preassign the right to join computers to the domain. This automatically provides the user with the Create/Delete Computer Objects permission. You can also do this by explicitly adding the Create Computer Objects and Delete Computer Objects permissions to the user within the **Computers** container of the appropriate domain or organizational unit in Active Directory.

By pre-assigning prestaged client computers with the right to join a domain, you enable users to turn on their systems, connect to a RIS server, log on with their domain accounts, and perform an unassisted installation of an operating system image — all without compromising the security of your network.

For this part of your RIS server security design process, use the “RIS Server Security” section of job aid “Designing the RIS Server Configuration” (ACIRIS\_09.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Server Configuration” on the Web at <http://www.microsoft.com/reskit>) to indicate whether you want to secure non-prestaged RIS clients by giving them the right to join a domain using the Active Directory **Delegation** feature.

### **Designing an optimal security configuration with prestaged clients**

You can optimize RIS server security by using prestaged clients. After you prestage computer accounts in Active Directory, configure your RIS server to only respond to these prestaged clients. To further enhance security, you can configure your users with read, write, and reset or change password permissions on the prestaged computer account objects.

For this part of your RIS server security design process, use the “RIS Server Security” section of job aid “Designing the RIS Server Configuration” (ACIRIS\_09.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Server Configuration” on the Web at <http://www.microsoft.com/reskit>) to record your decision to enhance the security of prestaged clients by setting user permissions on the prestaged computer accounts. Also indicate the user groups you want to receive these permissions.

### Designing the RIS server authorization method

To ensure that your RIS clients are serviced by known RIS servers on the network, you must authorize each RIS server. This ensures that the RIS server is recognized in Active Directory.

The easiest way to authorize RIS on a computer running Windows Server 2003 is to use the **Verify Server** feature on the **Remote Install** tab of the RIS server **Properties** dialog box. You can also type the following command at the command line:

```
Rissetup /Check
```

If you intend to delegate this task to specific personnel, they must be part of the Enterprise Admins security group or another group that you configure with this permission in order to access and configure a RIS server.

Alternatively, you can authorize a RIS server to Active Directory by using the **Authorize** function in the **Manage Authorized Servers** dialog box in the Windows Server 2003, Windows XP, or Windows 2000 DHCP snap-in.

To use the DHCP snap-in to authorize the RIS server, it is unnecessary to install the DHCP service. You can use this snap-in if the Administrative Tools package is installed on a computer running Windows XP Professional or Windows Server 2003, from which you can authorize the RIS server. You can install this package by running the adminpak.msi installer — located in the System32 directory of a computer running Windows Server 2003 — on the computer running Windows XP Professional.

You should not attempt to install Windows Server 2003 DHCP on a RIS server just to obtain the snap-in. To service RIS clients, any combined Windows Server 2003 DHCP/RIS server must have a fully functional DHCP service with defined and active scopes. This is because the Windows Server 2003 DHCP service on a combined server is aware that RIS is also present. If a client requests DHCP and remote boot services in its DHCP discovery broadcast, DHCP issues a single reply containing the specific details on DHCP and remote booting for that server. If the Windows Server 2003 DHCP service is not answering clients properly, the server does not generate a remote boot reply to clients requesting service.

For this part of your RIS server security design process use the “RIS Server Security” section of job aid “Designing the RIS Server Configuration” (ACIRIS\_09.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Server Configuration” on the Web at <http://www.microsoft.com/reskit>) to record the following information:

- The names of RIS server authorization personnel, who are either included in the Enterprise Admins group or in a separate RIS authorizers group that has appropriate permissions.
- The RIS server authorization location.

- The RIS server authorization method.
- Whether you need to install the Administrative Tools package on a computer running Windows XP Professional.

If you have multiple RIS servers, you might simplify things by using a common location and authorization method for each one. For example, you can choose to authorize all RIS servers from a remote administration session by using the **Verify** button in RIS server **Properties**.

---

## Designing the Active Directory Infrastructure

The successful implementation of RIS in your environment requires you to carefully analyze your Active Directory architectural design. The logical structure of Active Directory is separate and distinct from the physical network structure. You use physical structures to configure and manage network traffic. You use the logical structure of Active Directory to organize your network resources.

The core units of logical structure in Active Directory are forests, trees, domains, and organizational units. Forests consist of multiple trees which in turn consist of multiple domains that share a contiguous namespace. For any given domain, Active Directory provides organizational units, which are containers that you can use to organize users, computers, and resources into logical administrative groups. This can assist you when defining your RIS server location in Active Directory.

The core units of physical structure associated with Active Directory are sites, which consist of one or more Internet Protocol (IP) subnets connected by a high-speed link. Sites map the physical structure of a network; domains map the logical structure of your organization. Active Directory allows multiple domains in a single site and multiple sites in a single domain.

For further information about Active Directory planning and deployment, see “Designing the Active Directory Logical Structure” in *Designing and Deploying Directory and Security Services* of this kit.

### Choosing the Active Directory Location for RIS Servers

Where you place your RIS servers in Active Directory depends in part on how many clients you need to provide with RIS services. The Active Directory location you choose might also depend on your existing infrastructure. If you have a domain containing subnets that each have 75 clients or less, you might create an infrastructure with organizational units for each subnet to be serviced by a single RIS install server. Otherwise, for domains with 75 clients or less, you can use a single RIS install server to provide service to domain clients. Also, to simplify administrative organization, you can choose to create a logical grouping of your RIS servers by placing them all in the same organizational unit.

If it is not possible to locate your clients in close physical proximity to your RIS server, you might locate a RIS server at a particular site and allow RIS clients to connect to it remotely to receive remote installation services. If RIS servers and clients are at different Active Directory sites on separate IP subnets in a common domain, you must connect them with a high speed links, such as a fiber optic backbone. This ensures adequate installation times and minimal traffic congestion during periods when RIS is active.

For this part of your Active Directory infrastructure design process, use the “RIS Network Deployment Configuration” section of job aid “Designing the RIS Server Configuration” (ACIRIS\_09.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Server Configuration” on the Web at <http://www.microsoft.com/reskit>) to record the Active Directory location of each RIS server.

### **Designing Active Directory Support**

To design the Active Directory configuration that supports RIS, you need to define the following:

- Any new Active Directory security groups you want to provide for RIS administrators.
- The details of prestaging RIS clients in Active Directory.

#### **Defining new Active Directory security groups**

If you decided to delegate RIS administrative tasks in job aid “Planning RIS Server Security” (ACIRIS\_05.doc), you need to create a new group in Active Directory for RIS administrators. For more information about delegation issues see “Planning Security for RIS Administrative Tasks” earlier in this chapter. If you want to designate more than one group with each handling different tasks, you need to create multiple security groups. After you create the groups, you need to set the appropriate permissions to allow performance of assigned tasks.

For this part of your Active Directory design, use the “Designing Active Directory Support” section of job aid “Designing the RIS Server Configuration” (ACIRIS\_09.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Server Configuration” on the Web at <http://www.microsoft.com/reskit>) to finalize your decision to create Active Directory security groups for RIS administrators or add administrative personnel to the Enterprise Admins group. If you decide to create new groups, record the names of the groups and the personnel you want to add to them.

### Defining prestaging details

You can prestage client computer accounts either manually using the Active Directory snap-in or with the prestaging script from the Remote Installation Scripts link on the Web Resources page (<http://www.microsoft.com/windows/reskits/webresources>). If you have a small number of clients, it might be sufficient to use the snap-in. If you use the snap-in, however, you can only configure the computer name, UUID, and the RIS server you choose to support the client. You cannot specify which startup file is designated for each client, as you might want to do when configuring some clients with automated installations and others with interactive installations. However, you can designate the startup file by using the prestaging script.

While the primary use of the prestaging script is to automate the prestaging process, you can also use it to automate the configuration of startup boot files for client use. Automating this process helps reduce administrative efforts in a large environment. However, for the prestaging script to work properly, you must run it from within the domain where you want to prestage clients, and the computer from where you run it must have ADSI installed.

The prestaging script uses an Excel spreadsheet created by the BIOS information script as input data, as described in “Evaluating the RIS Client Prestaging Process” earlier in this chapter. You run the BIOS information script to automate the process of obtaining the UUIDs of existing client computers on your network for prestaging these computer accounts in Active Directory.

If you have an OEM spreadsheet with the UUIDs of new client computers, you can add this information to the second column of the Excel spreadsheet generated by the BIOS information script. The OEM UUIDs that you add to the spreadsheet must each be a 32-bit hexadecimal number in raw byte order format as follows:

1534A67812B41C34123F12365E432D16



#### Note

When you prestage manually using the Active Directory snap-in, you can use either the raw byte or *pretty print* format. Pretty print format includes curly braces and spaces, as follows:

```
{12345678-1234-1234-1234-15E4160B15F2}
```

When you add OEM UUIDs to the spreadsheet, you must also add other information, including the new computer account name, location, domain\user, description, and startup boot file path. See the prestaging script for more information. The startup boot file path is the path to the RIS server location where the boot files are located, for example:

```
\\RIServername\REMINST\OSChooser\i386\Startrom.n12
```

In the spreadsheet, you can specify which startup file you want for each client, by using either the Startrom.n12 or Startrom.com boot files. However, the prestaging script also provides options that allow you to set all clients to either boot file, to accommodate groups of clients that you configure with interactive or automated installations. When you choose to use these options, you must specify the appropriate action command, the RIS server name, the image name, and the path to a fully-configured input spreadsheet file. In this case, the script does not read data from the cells in Startup File Path column of the spreadsheet, but applies the value you enter at the command line to each client computer account listed in the spreadsheet. Values are **automate**, to configure the client with Startrom.n12 and **interactive**, to configure the client with Startrom.com.

The prestaging script contains usage instructions that explain how to run the script and the commands or input arguments you must provide. The script also provides header information that explains the details of the Excel spreadsheet file format. Whether you prestage by script or manually, you still must acquire the UUIDs for your client computers. For more information about methods to acquire the UUIDs for client computers, see “Evaluating the RIS Client Prestaging Process” earlier in this chapter.

For this part of your Active Directory design, use the “Designing Active Directory Support” section of job aid “Designing the RIS Server Configuration” (ACIRIS\_09.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Server Configuration” on the Web at <http://www.microsoft.com/reskit>) to record your decision to prestage client computers in Active Directory either manually or using the prestaging script. If you decide to prestage, also record the name of the input Excel file that the script requires and the personnel who will create and configure this file. You can also specify the method you will use to obtain UUIDs.

---

## Designing a Test RIS Environment

Before implementing a full scale RIS deployment in your organization, you can create a RIS test environment to facilitate preliminary RIS configuration and testing. After confirming that the test environment produces the desired results, you can begin your RIS rollout. For more information about creating a test environment, see “Designing a Test Environment” in *Planning, Testing, and Piloting Deployment Projects* of this kit.

The RIS test environment enables you to create and configure your RIS server, generate operating system images, and perform test deployments of RIS images to clients outside your production environment. You can also use the RIS test environment to run tests on uniquely tailored answer files and custom CIW configurations to assure proper functioning prior to introducing them in your network. You might also use your test environment to do a preliminary test run of the BIOS information, prestaging and boot file name scripts to become familiar with them before running them on the network. In addition, you can use the RIS test environment to acquire baseline performance indications for your RIS server. For more information about RIS server performance, see “Planning RIS Server Performance” earlier in this chapter.



To create the RIS test environment, you need a minimum of two computers. You can set up one computer as a domain controller with multiple roles, including Active Directory, DNS, DHCP, and RIS, and a second computer that serves as a master computer from which you create custom file system images using Riprep. After you configure one or more images and place them on the RIS server, you can use the second computer as a client on which you install the image. Also, if you want to create CD-type operating system images in your test environment and you have the operating system CDs, you can run Risetup on the RIS server.

Alternatively, you can use a three-computer configuration such as the following:

- One domain controller with Active Directory, DNS, and DHCP.
- One member server on which you install RIS.
- One combined master and client computer running the operating system you want to image, such as Windows XP.

If you have additional computers, you can break up the combined master and client configuration and provide separate computers for each. This simplifies things because you can avoid repeated installations of operating systems on the master computer after performing test installations on the client with RIS.



### Important

In your production environment, strongly consider not having your domain controller share multiple roles. Instead, you can configure separate computers with unique roles such as domain controller with DHCP, member server with Active Directory and DNS, and member server with RIS.

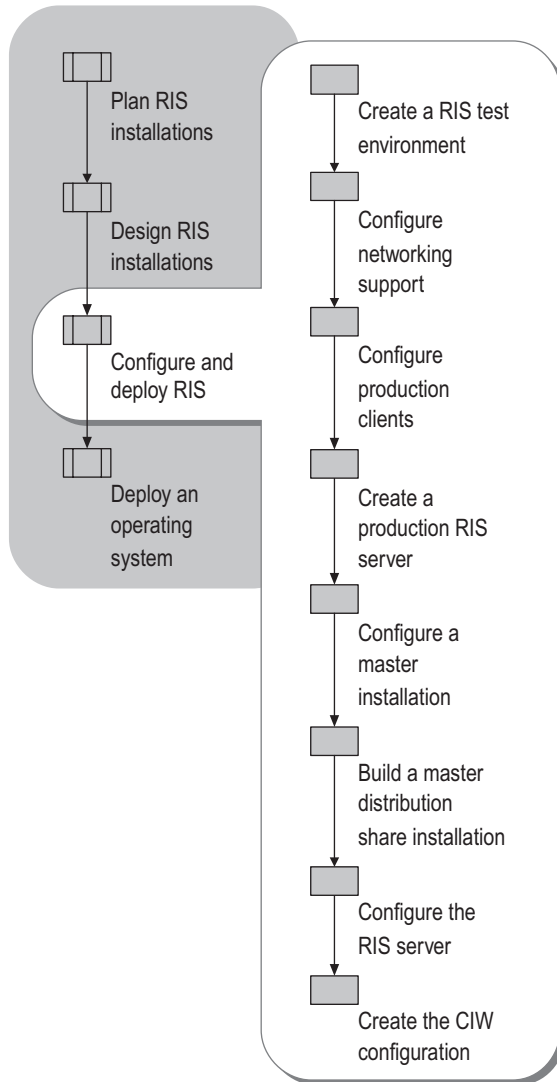
For this part of your design process, use job aid “Designing a RIS Test Environment” (ACIRIS\_10.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing a RIS Test Environment” on the Web at <http://www.microsoft.com/reskit>) to record the configuration of your test environment and the tasks you intend to carry out there, including any of the following:

- Configuring your test RIS server.
- Testing-run scripts for prestaging, getting client UUIDs, and changing startup file names.
- Creating operating system images using Riprep and Risetup.
- Testing answer files and CIW configurations in trial deployments.
- Analyzing RIS server performance.

## Configuring and Deploying RIS

At this point, you can pass your design job aids to the deployment team to serve as inputs to the RIS configuration and deployment process. Figure 4.8 illustrates the order of the configuration and deployment tasks to accomplish at this stage.

**Figure 4.8 Configuring and Deploying RIS**



For specific procedures that support the RIS configuration and deployment process, see “Remote Installation Services” in Help and Support Center for Windows Server 2003.

## Creating a RIS Test Environment

To create a RIS test environment for running preliminary tests, you need to accomplish the following tasks:

- 1.** Install the appropriate hardware on your RIS server to support your test environment and then install the Windows Server 2003 operating system.
- 2.** Install RIS on your test RIS server. (This automatically creates a CD-type Risetup image.)
- 3.** Create any additional Risetup images using operating system CDs.
- 4.** Install the appropriate hardware on a computer you designate as a domain controller for your RIS test environment and then install the Windows Server 2003 operating system.
- 5.** Install Active Directory by running `dcpromo.exe` at the command line or by running the Active Directory Installation Wizard.
- 6.** Configure and activate your DHCP scope to provide IP addresses on the test network.
- 7.** Install the appropriate hardware and the Windows XP Professional operating system on a computer you designate in the role of master computer and RIS client.
- 8.** Connect the domain controller, RIS server, master computer and RIS client to the test network using linear bus topology and Ethernet components.
- 9.** Configure Active Directory on the domain controller with user and computer accounts and join the RIS server and client to the test domain. (You can prestage the client computer account using the UUID of the client computer.)
- 10.** Install and configure applications on the master computer, set operating system parameters, and add any special drivers required for a Riprep image.
- 11.** Create the Riprep image on your RIS server by running `Riprep.exe` from the master computer.
- 12.** Create any custom answer files (including permissions) and CIW configurations.
- 13.** Configure your test RIS server with client support options, a computer naming format, and the location where computer accounts are generated.
- 14.** Reinstall an operating system on the master computer, which now acts as the client.
- 15.** If you configure the RIS server for automated installations, set the boot sequence in the BIOS of client computers to boot from the hard disk first and the network boot device second.
- 16.** Disable any active boot partitions on the client computer hard disk using a tool such as `Diskpart.exe`.

To run preliminary tests, perform the following tasks:

1. Test-run the scripts for obtaining client UUIDs, prestaging clients in Active Directory, and changing startup file names.
2. Test custom answer file, CIW, and boot configurations in trial operating system deployments.
3. Analyze RIS server performance.

After you achieve the results you expect in your RIS test environment, proceed to the configuration tasks for your production environment.

---

## Configuring Networking Support

You need to configure your domain controller to support the RIS server that provides operating system installation services. You also need to configure your network infrastructure to support RIS-based operating system installations.

### Configuring Domain Controller Support

To configure your domain controller, you need to accomplish the following:

1. Install the appropriate hardware on your domain controller to support the RIS environment and then install the Windows Server 2003 operating system.
2. Ensure that you have the software required to support RIS, including:
  - DHCP installed and activated on your domain controller, unless you are using a third-party application on a member server.
  - A configured DNS server to provide name resolution services for the domain.
3. Add a RIS installation account to your domain to enable autologon. Use the Active Directory Users and Computers snap-in to create this account.

### Network Infrastructure Configuration

To configure your network infrastructure, you need to accomplish the following:

1. Make any necessary changes to your network topology to provide support for the minimum data transmission rate of 10 Mbps (100 Mbps is highly recommended). See “Assessing the Network Infrastructure” earlier in this chapter.
2. Ensure that you have the necessary components in your network to support RIS, including a domain controller running Windows Server 2003 with DHCP and Active Directory services, and a DNS server. See “Assessing RIS Server Software Requirements” earlier in this chapter.

3. Install your RIS servers at suitable network installation points. See “Evaluating Network Installation Points” earlier in this chapter.
4. Set the NTLM authentication level you require on the network. See “Evaluating the NTLM Authentication Level” earlier in this chapter.
5. Set up standard security measures for your network, including auditing and monitoring, securing physical access to the network, and enforcing a strict password policy. See “Assessing the Security of the PXE Environment” earlier in this chapter.

---

## Configuring Production Clients

To configure production clients in preparation for RIS-based operating system installations, you need to accomplish the following:

1. Install new client computers that use the correct hardware to support RIS installations in the appropriate locations on your network. See “Evaluating RIS Client Hardware” earlier in this chapter.
2. Install the correct hardware on existing clients to support RIS installations. See “Evaluating RIS Client Hardware” earlier in this chapter.
3. Update any existing client computers that have incorrect HAL types for the Riprep images they are to receive. For more information about verifying the RIS client remote boot configuration, see “Evaluating Remote Boot Capabilities of RIS Clients” earlier in this chapter.
4. Run the BIOS information script to determine client BIOS compatibility with network adapter booting. For more information about verifying the RIS client remote boot configuration, see “Evaluating Remote Boot Capabilities of RIS Clients” earlier in this chapter.



### Note

Before running the BIOS information script, you must ensure that the computer running the script has ADSI and WMI installed and that client computers have WMI installed.

5. Create RIS boot floppy disks for non-PXE enabled clients. For more information about verifying the RIS client remote boot configuration, see “Evaluating Remote Boot Capabilities of RIS Clients” earlier in this chapter.
6. Migrate user state. For more information about migrating user state, see “Auditing Existing Clients” earlier in this chapter.

7. Obtain client computer UUIDs, using either Systems Management Server, OEM listings, or run the BIOS information script. For more information about obtaining client computer UUIDs, see “Evaluating the RIS Client Prestaging Process” earlier in this chapter.
8. For PXE-enabled clients receiving an automated installation, configure the boot sequence in the BIOS to boot from the hard disk first and the network adapter second.
9. For non-PXE enabled clients receiving an automated installation, configure the boot sequence in the BIOS to boot from the hard disk first and the floppy disk second.
10. Disable all active boot partitions on the hard disk of all client computers receiving an automated installation by using a tool such as Diskpart.exe with the /S:disablepart.txt argument.
11. Erase the hard disks of client computers using a management application such as Systems Management Server.

For more information about defining the boot configuration, also see “Fully-Automated Installation Design Tasks” earlier in this chapter.

---

## Creating a Production RIS Server

To create a production RIS server to provide operating system installation services on the network, you need to accomplish the following:

1. Install the hardware necessary on each server to support RIS installations. For more information about RIS server hardware requirements, see “Evaluating RIS Server Hardware Requirements” earlier in this chapter.
2. Install the Windows Server 2003 operating system on each RIS server. For more information about RIS server software requirements, see “Assessing RIS Server Software Requirements” earlier in this chapter.
3. Install RIS on each RIS server. For more information about RIS components and deploying RIS, see “Process for Deploying RIS” earlier in this chapter.
4. Create any additional Risetup images for the RIS servers using operating system CDs. For more information about choosing additional Risetup images to host on RIS servers, see “RIS Server Configuration Design Tasks” earlier in this chapter.



### Note

You can join the RIS server to the domain where it will provide service after you configure domain controller support.

## Configuring a Master Installation

To configure a master computer from which you generate Riprep images, you need to accomplish the following:

1. Install the appropriate hardware and the Windows XP Professional operating system on a computer you designate as the master computer and join it to the domain where the RIS server is located. For more information about master computer hardware requirements, see “Assessing Master Computer Requirements” earlier in this chapter.
2. Install and configure applications on the master computer, set operating system parameters, and add any special drivers required for a custom Riprep image. For more information about designing Riprep images, see “Design a Riprep-Based Installation” earlier in this chapter.
3. Test your Riprep images to determine the impact on user profiles. For more information about how Riprep image design affects user profiles, see “Riprep Image Design and User Profiles” earlier in this chapter.
4. Create the Riprep image on your RIS server by running Riprep.exe from the following location: `\\rissserver\\reminst\\admin\\i386\\riprep.exe`.
5. Configure permissions on the answer files for each Riprep image you create and on the operating system image folders, to allow users to access the images. For more information about setting permissions on answer files, see “Evaluating Security for Operating System Images” earlier in this chapter.



### Note

If you set the local administrator password on a Riprep image, passwords entered in the CIW are ignored.

---

## Installing the Master Computer Operating System

When you install the operating system on the master computer, use the unattended method. By using unattended installs, it is easier to create and catalog unique configurations of operating systems that include different components such as drivers and applications. For each operating system installation, you create a separate answer file that identifies the components of the master installation configuration. The answer file facilitates the unattended installation and also serves as a record of your master operating system installation configuration, which is easily stored and can be used to re-create the original configuration.

Another benefit of using an unattended installation for your master computer configuration is that you can include a command in the GUIRunOnce section of the answer file to automatically start Riprep.exe when the unattended installation completes. By integrating Riprep into the unattended installation, you automatically create the master installation image on your RIS server.

For example, creating a master installation for a file server using an unattended installation with Riprep involves the following steps:

1. Create an answer file and configure it with entries and values for components that are appropriate for your master operating system configuration.
2. Specify the command to run Riprep.exe in the GUIRunOnce section of the answer file by using the following entry:

```
[GuiRunOnce]
```

```
"\\rissserver\\reminst\\admin\\i386\\riprep.exe"
```

3. At a command prompt on the server, use the following syntax to run the unattended installation:

```
Winnt32.exe /unattend: answerfilepath
```

For more information about creating answer files for unattended installations, see "Answer files" in *Microsoft Windows Server 2003 Corporate Deployment Windows Corporate Deployment Tools User's Guide* (Deploy.chm). Deploy.chm is included in the Deploy.cab file in the Support folder on the Windows Server 2003 operating system CD.

---

## Configuring the Master Computer Operating System

To configure the master computer, you need to accomplish the following:

1. Create the desktop configuration.
2. Add hardware devices.
3. Set passwords.
4. Create an optional command file.
5. Set language and regional options.
6. Add and configure applications

You must also clean up the installation by doing the following:

**Reset history settings** Reset all history settings in the operating system and all applications that are installed on the master installation. This includes the most frequently used applications list and the history list in Internet Explorer.



**Delete files and folders** Delete all files and folders that you do not want end users to see. This might include:

- Files and folders that you used to build the master installation, such as tools, documents, and scripts.
- Temporary Internet files, including cookies.
- Files and folders in My Documents.

**Configure the user profile for the Default User** Configure the user profile for the Default User so that all of the installation and configuration tasks you performed are available to end users. To do this, you first create a local user account, and then add the account to the local Administrators group. Next, log on to the computer using the new user account, and copy the Administrator user profile to the Default User profile. Do not log off.

---

## Testing Riprep Images and User Profiles

When creating Riprep images, you need to understand how user profiles affect the changes you make to a master installation and the impact on users who log on to computers that receive the Riprep image.

Applications that are compliant with the operating system that you are preparing to deploy properly separate user-specific and computer-specific configuration settings and data. Installing such applications in your Riprep master installation makes them available to all users of client computers on which you install the Riprep image. Applications that are not compliant with Windows Server 2003 might rely on per-user configurations that are specific to the profile of the user (typically the Administrator) who actually installs the applications prior to running Riprep, rather than computer-specific configurations. These configurations remain specific to the installing user, which can result in the application or configuration setting not being available or not functioning properly for the users of the client computer where you install the Riprep image. Also, some non-application configuration changes, such as the wallpaper specified for a user's desktop, are applied only to the current user's profile by default, which means they are not available to users of the client computer where you install the Riprep image.

To ensure that the application or configuration settings of your Riprep image work properly with the implementation of user profiles in your organization, you need to test them thoroughly. To test a configuration, you can make a change while logged on as the Administrator, log off, and then log on with a user account that is representative of your organization. If the change you made applies to the user account with which you log on, then it should also apply to all users who log on to systems installed with a Riprep image containing the same change. Complete your testing by creating a Riprep image and installing it on a client computer. Log on to the computer with a different user account and verify that the change applies and is fully functional.

## Running the Riprep Wizard on the Master Computer

When you are ready to create your image, you run Riprep.exe from the master computer by specifying the following in the **Run** dialog box:

```
\\RISServerName\Reminst\Admin\i386\Riprep.exe
```

By default, Riprep-based images do not perform full Plug and Play enumeration during operating system installation on the client. If you want full Plug and Play enumeration to occur, you must start Riprep.exe with the **/pnp** option, as follows:

```
\\RISServerName\Reminst\Admin\i386\Riprep.exe /pnp
```

After you run this command, full Plug and Play enumeration occurs. If you want to turn off full Plug and Play enumeration, you must recreate the image.



### Note

You can also run Riprep.exe by entering these commands at the command line.

## Replicating Images to Other RIS Servers

RIS does not provide a mechanism for replicating operating system images from one RIS server to another. However, you can use third-party tools to replicate operating system images. If you use a third-party tool, make sure that the replication mechanism supports alternate file streams, file maintenance attributes, extended attributes, and security settings of the source images.

---

## Configuring Answer File and Image Folder Permissions

Each time you run Riprep.exe on a master installation, you create a default answer file that is specifically configured for that master image. To make this image available to your users, you must set Read permissions on the answer file associated with it. Using the **Images** tab in RIS server **Properties**, set the ACL on each answer file to specify which users can receive the master installation image. Note that you also need to set Read permissions on the operating system image folder located in the following directory path on the RIS server:

```
\\RISServer\RemoteInstall\Setup\LanguageFolder\Images\OSImageFolder\
```

Setting permissions on the image folder ensures that specified users will have access to the operating system image.

## Building a Master Distribution Share Installation

When you create your RIS server on a computer running Windows Server 2003, you also automatically create an initial CD-type image of Windows XP Professional or Windows Server 2003. However, you can also create additional CD-type images. To create a CD-type image of an operating system on a RIS server from which you can build custom distribution share installations, you need to accomplish the following:

1. Log on to the RIS server.
2. Insert a CD of the operating system you want to image in the CD-ROM drive of the master computer.
3. Locate your RIS server by using the Active Directory extension.
4. Use the **Add** button on the **Images** tab of your RIS server **Properties** dialog box to run the **Remote Installation Services Setup Wizard** (Risetup), which locates the operating system source files and creates the directory structure of the image.
5. Install applications and drivers in your distribution share.
6. Configure new answer files that create unique operating system installations by using `Cmdlines.txt` and the entry `[GUIRunOnce] unattended`.

For more information about designing a Risetup image, including configuring custom answer files, see “Design a Risetup-Based Installation” earlier in this chapter.

---

## Configuring the RIS Server

By configuring your RIS server, you determine the way it responds to RIS clients requesting service. If your design includes a RIS referral server, your configuration options are slightly different.

### RIS Server Configuration

To configure your RIS server, you need to accomplish the following tasks:

1. Authorize the RIS server to Active Directory using the **Verify** button on the **Remote Install** tab of your RIS server **Properties** dialog box.
2. Set client response options that determine whether the RIS server responds to all clients requesting service or only to those that have prestaged computer account objects in Active Directory.
3. Set the computer naming policy.

4. Set the location where new managed computer account objects will be created in Active Directory.
5. Set permissions for RIS users to create computer accounts using the **Delegation** feature of Active Directory to preassign them the right to join computers to the domain. Alternatively, do this by explicitly adding the Create Computer Objects and Delete Computer Objects permissions to the client within the **Computers** container of Active Directory.
6. If you are prestaging client computers in Active Directory, add prestaged computer accounts to the domain by using the Active Directory extension on your RIS server or automate the process by running the prestaging script from any domain computer that has ADSI and WMI installed.
7. Using the **Images** tab of your RIS server **Properties** dialog box, associate any additional answer files you have with Riprep and Risetup images that are located on the RIS server.

**Note**

Any configuration changes you make from the Active Directory extension on your RIS server might not be immediately replicated to other domain controllers in Active Directory. The time required to replicate changes depends on your network topology.

## RIS Referral Server Configuration

To configure a RIS server as a referral server, you need to accomplish the following tasks:

1. Install the hardware required to support the Windows Server 2003 operating system on the computer you designate as a RIS referral server.
2. Install RIS as described above and at least one CD image.
3. Authorize the RIS referral server to Active Directory using the **Verify** button in your RIS server **Properties** dialog box.
4. Set the **Do not respond to unknown client computers** option in the RIS server **Properties** dialog box.

**Note**

The RIS referral server only acts in the capacity of making referrals if you prestage clients in Active Directory and configure them to use specific RIS install servers.

## Creating the CIW Configuration

If you are using the default CIW configuration, you do not need to perform any of the following configuration tasks. Otherwise, to create a custom CIW configuration, you need to accomplish the following:

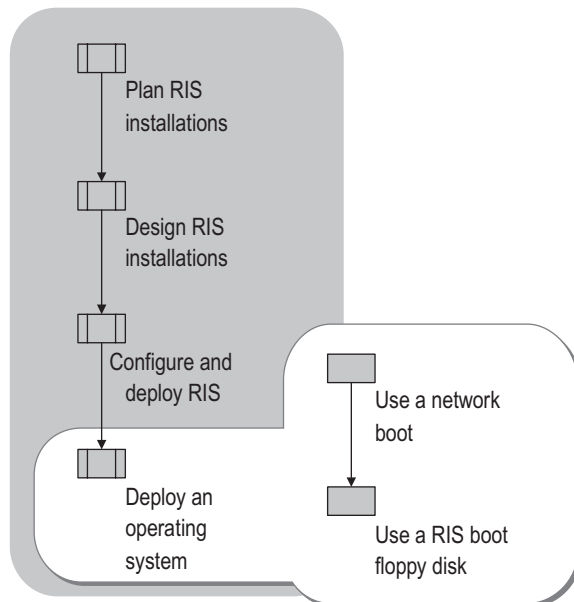
1. If you have not done so already, configure the operating system installation options you want to present to clients by setting answer file ACLs to permit or deny client access to operating system images in the CIW.
2. If you have not done so already, configure permissions for the operating system image folder on the RIS server to explicitly deny access to specific user groups, if applicable.
3. Configure the setup options you want to provide to RIS clients by configuring RIS-related settings in the default domain Group Policy or in any new Group Policy objects that you create for specific user groups.
4. Modify existing screens and use OSCML tags to create custom input prompts.
5. Add any new screens you want and use OSCML tags to create custom input prompts or information displays.
6. Configure answer files with OSC variables to capture user input.
7. Remove screens from the CIW by modifying the <FORM ACTION="screenname"> tags with different screen names, as required.
8. Add any language options to the CIW by modifying the Welcome screen.

For an OSCML tag reference, see job aid "OSCML and Client Installation Wizard Variables" (ACIRIS\_13.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see "OSCML and Client Installation Wizard Variables" on the Web at <http://www.microsoft.com/reskit>). For more information about Group Policy settings that affect the CIW in addition to using OSCML tags and OSC variables, see "CIW Design Tasks" earlier in this chapter.

## Deploying an Operating System

Once you have completed configuring and deploying RIS in your production environment, you are ready to perform operating system deployments in your production environment. Figure 4.9 illustrates the deployment options at this stage of the process.

**Figure 4.9 Deploying an Operating System**



To deploy an operating system by using RIS requires that client computers initiate a remote network boot. To do this, you must use one of the following methods:

- Use PXE-enabled client computers to boot from their network cards to a remote RIS server.
- Use a RIS boot floppy disk to emulate the PXE process to boot supported non PXE-enabled client computers from a remote RIS server.

---

## Using a Network Boot

To perform deployment of an operating system image hosted on a RIS server using a network boot from a PXE-enabled client, you need to accomplish the following:

1. Power up the client computer.
2. If the client is receiving an interactive deployment, wait for the client to receive a prompt to press the F12 key for a network boot to a RIS server. The prompt appears after the client receives an IP address from the DHCP service.

3. Press the F12 key to initiate the network boot.
4. If the client is receiving an automated deployment, wait for the CIW to begin downloading. The download begins after the client receives an IP address from the DHCP service. The F12 prompt is bypassed for automated deployments.
5. Follow the CIW screens after TFTP downloads the CIW files to the client.

---

## Using a RIS Boot Floppy Disk

To perform deployment of an operating system image hosted on a RIS server using a network boot from a RIS boot floppy disk client, you need to accomplish the following:

1. Insert the RIS boot floppy disk into the client computer floppy disk drive.
  2. Accomplish the tasks listed in the previous section “Using a Network Boot.”
- 

# Additional Resources

These resources contain additional information related to this chapter.

### Related Information

- “Designing the Active Directory Logical Structure” in *Designing and Deploying Directory and Security Services* of this kit for information about Active Directory planning and deployment.
- 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 an introduction to TCP/IP, or for more information about Dynamic Host Configuration Protocol (DHCP).
- 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 the Windows Installer, and about using Group Policy to configure computer and user deployments of applications.
- “Migrating User State” in this book for information about migrating user data and settings.

### 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.

- “Operating Systems supported by Remote Installation Services” in Help and Support Center for Windows Server 2003 for more information about operating systems supported by RIS.
- “Remote Installation Services system requirements” in Help and Support Center for Windows Server 2003 for more information about Remote Installation Services system requirements.

- “Remote Installation Services administration overview” in Help and Support Center for Windows Server 2003 for procedures to prestage RIS clients using the Active Directory snap-in on a RIS server.
- “Setting the LAN Manager Authentication Level on a network that includes RIS” in Help and Support Center for Windows Server 2003 for more information about choosing the most appropriate LAN Manager authentication level in a network that includes RIS.
- “Set permissions for administrators who manage client installation images for RIS” in Help and Support Center for Windows Server 2003 for more information about permission requirements for RIS tasks.
- “Remote Installation Services” in Help and Support Center for Windows Server 2003 for specific procedures that support the RIS configuration and deployment process.

**Related Job Aids**

- “Planning for RIS Clients” (ACIRIS\_01.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning for RIS Clients” on the Web at <http://www.microsoft.com/reskit>).
- “Planning for RIS Servers” (ACIRIS\_02.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning for RIS Servers” on the Web at <http://www.microsoft.com/reskit>).
- “Planning the Master Computer Configuration” (ACIRIS\_03.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning the Master Computer Configuration” on the Web at <http://www.microsoft.com/reskit>).
- “Planning the RIS Network Configuration” (ACIRIS\_04.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning the RIS Network Configuration” on the Web at <http://www.microsoft.com/reskit>).
- “Planning RIS Server Security” (ACIRIS\_05.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Planning RIS Server Security” on the Web at <http://www.microsoft.com/reskit>).
- “Defining Riprep Images” (ACIRIS\_06.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Defining Riprep Images” on the Web at <http://www.microsoft.com/reskit>).
- “Defining Risetup Images” (ACIRIS\_07.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Defining Risetup Images” on the Web at <http://www.microsoft.com/reskit>).
- “Designing the RIS Deployment Mode and CIW Process” (ACIRIS\_08.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Deployment Mode and CIW Process” on the Web at <http://www.microsoft.com/reskit>).



- “Designing the RIS Server Configuration” (ACIRIS\_09.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing the RIS Server Configuration” on the Web at <http://www.microsoft.com/reskit>).
- “Designing a RIS Test Environment” (ACIRIS\_10.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Designing a RIS Test Environment” on the Web at <http://www.microsoft.com/reskit>).
- “The CIW Process” (ACIRIS\_11.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “The CIW Process” on the Web at <http://www.microsoft.com/reskit>).
- “Reserved OSC Variables” (ACIRIS\_12.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “Reserved OSC Variables” on the Web at <http://www.microsoft.com/reskit>).
- “OSCML and Client Installation Wizard Variables” (ACIRIS\_13.doc) on the *Windows Server 2003 Deployment Kit* companion CD (or see “OSCML and Client Installation Wizard Variables” on the Web at <http://www.microsoft.com/reskit>).
- The Remote Installation Scripts link on the Web Resources page <http://www.microsoft.com/windows/reskits/webresources> for the BIOS information script, the prestaging script, and the boot file name script.



# Migrating User State

5

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

<b>Overview of Migrating User State.....</b>	<b>296</b>
<b>Choosing a User State Collection Method.....</b>	<b>300</b>
<b>Identifying Migration Content.....</b>	<b>307</b>
<b>Creating a Detailed Migration Plan.....</b>	<b>311</b>
<b>Testing Your Migration Process.....</b>	<b>319</b>
<b>Additional Resources.....</b>	<b>321</b>

## Related Information

- For information about using Remote Installation Services (RIS), see “Designing RIS Installations” in this book.
- For information about scripting in a Microsoft® Windows® Server 2003 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.

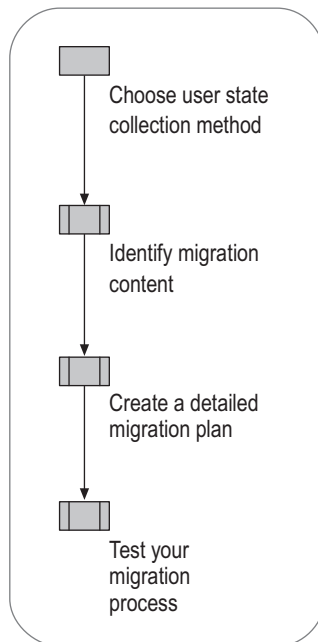
The degree to which an organization should automate user state migration depends on these and a variety of other factors, including the number of users to be migrated and how widely dispersed they are; how centralized the organization's IT effort is; the degree to which users share a common desktop, 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.

## 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 5.1 shows the process for planning a user state migration.

**Figure 5.1 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 System Tools. (On the Program 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 enables administrators to precisely configure unique settings, such as making user-specific modifications to the registry. The tool is included on the 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 5.1 and Table 5.2 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 5.1 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	.oqy	.sh3	Cookies
.wps	.rqy	.ch3	
.scd	.wk?	.pre	
.wri	.wq1	.ppa	
.wpd	.slk		

**Table 5.2 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, 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 link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

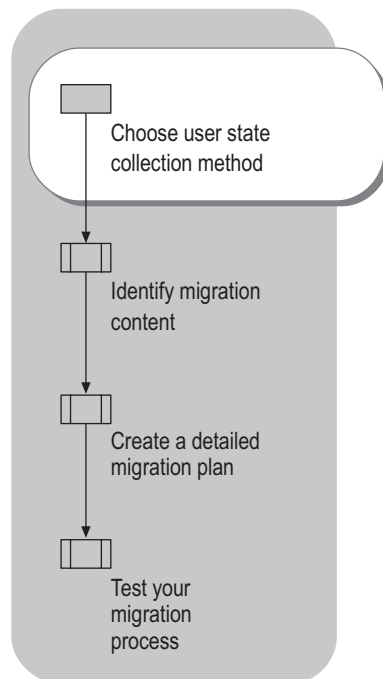
---

## 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 5.2). Four user state migration methods are available for collecting and restoring user state:

- Manual migration
- Scripted-manual migration
- Centralized automation
- User-driven migration

**Figure 5.2** Choosing a User State Collection Method





The method by which you deploy Windows XP affects which user state migration method you should choose. Table 5.3 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 5.3 Effects of Windows XP Deployment Methods on User State Migration**

Deployment Method	Effects on User State Migration
<b>Wipe-and-load.</b> 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.
<b>Parallel deployment.</b> 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.
<b>Operating system upgrade.</b> 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's 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 5.4 summarizes advantages and disadvantages of manually migrating user state. Because of the noted disadvantages, a strictly manual approach is not recommended.

**Table 5.4 Advantages and Disadvantages of Manual User State Migration**

Advantages	Disadvantages
<ul style="list-style-type: none"><li>▪ A technician is available to deal with unexpected problems.</li><li>▪ Users are reassured by having a person to ask questions of during the migration.</li></ul>	<ul style="list-style-type: none"><li>▪ Expensive because of high technical labor costs.</li><li>▪ Slow because a technician must visit each computer individually.</li><li>▪ Higher chance of human error than with automated methods.</li><li>▪ Does not scale to distributed or remote office scenarios.</li></ul>

## 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 5.5 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 5.5 Advantages and Disadvantages of Scripted-Manual User State Migration**

Advantages	Disadvantages
<ul style="list-style-type: none"> <li>▪ A technician is available to deal with unexpected problems.</li> <li>▪ Users are reassured by having a person to ask questions of during the migration.</li> <li>▪ Lower chance of human error than with a purely manual migration method.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Requires that a technician be onsite, with physical access to each computer that is being migrated.</li> <li>▪ Requires that script files be created.</li> <li>▪ Does not scale to distributed or remote office scenarios.</li> </ul>

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 5.6 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 5.6 Advantages and Disadvantages of Centrally Automating User State Migration**

Advantages	Disadvantages
<ul style="list-style-type: none"><li>▪ Allows simultaneous migration of user state for large numbers of computers (limited only by network bandwidth and server storage).</li><li>▪ Produces results that can be replicated.</li><li>▪ Produces a common user experience.</li><li>▪ Scales well to distributed or remote office scenarios.</li></ul>	<ul style="list-style-type: none"><li>▪ Requires that script files be created.</li><li>▪ Does not work well in parallel deployments.</li></ul>

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.
- Writing scripts that will create a temporary store for each user's state and then restore that state on the destination computer.
- Automatically deploying a Windows XP image on remote computers without user intervention.

**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, without user intervention at the remote computer during 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 an Automated Installation Method" in this book.

## 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 5.7 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.

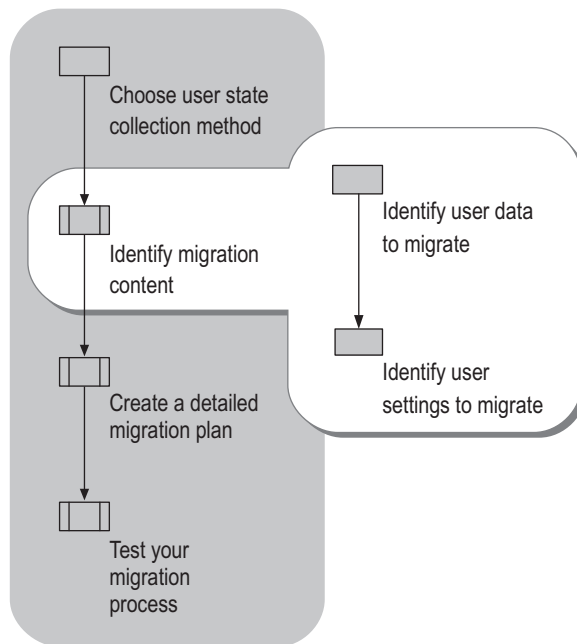
**Table 5.7 Advantages and Disadvantages of User-Driven User State Migration**

Advantages	Disadvantages
<ul style="list-style-type: none"> <li>■ Controlled tool better enables users to drive their own migration.</li> <li>■ Can use the data captured using customized .inf files.</li> </ul>	<ul style="list-style-type: none"> <li>■ IT staff are not involved in the actual migration; relies on the user's judgment.</li> <li>■ No standard storage location.</li> <li>■ Minimal control over what is migrated, resulting in a less standardized desktop.</li> </ul>

# 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 5.3. Consider which data and settings are worth migrating and which do not provide sufficient benefits to justify the cost of migration.

**Figure 5.3** 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 storage capacity 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 to determine which user data to migrate 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 migrate, 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 help 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`. You can use the Sysdiff.exe tool to compare images of the registry before and after migration. Sysdiff.exe finds updated registry entries. The Sysdiff.exe tool 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>.



### 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>.

## 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 5.8 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 5.8 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

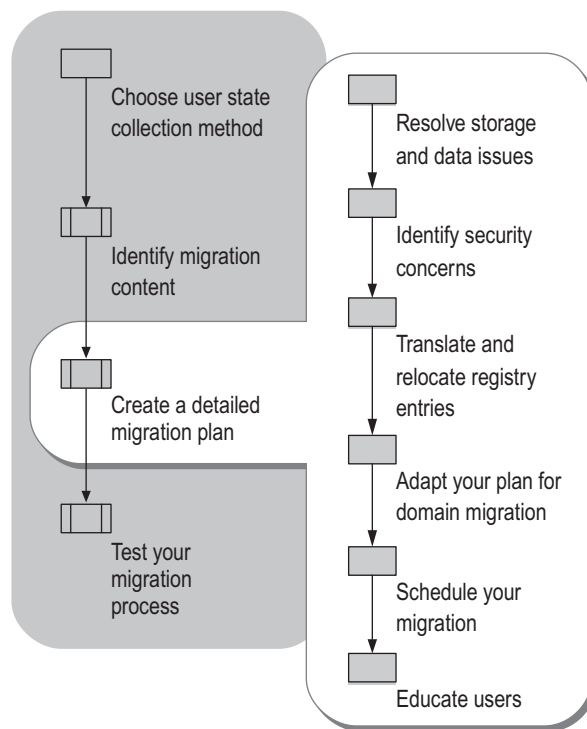
Less measurable, but equally important, is the time that IT professionals and the Help desk staff spend helping users reconfigure desktops when their personal settings are not migrated.

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 can decrease while users adjust these settings to suit 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. In your migration plan, include a migration schedule and detailed instructions for users. Figure 5.4 shows the tasks involved in creating a detailed plan for user state migration.

**Figure 5.4** 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 temporary 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 temporary 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 temporary storage location. To enhance performance, locate the temporary store on high-speed drives. Ensure that the temporary storage of user state is the only task that the store performs and that it has an optimized (high-speed) network connection.

**E-mail** 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 megabytes (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 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 “Tools Used in the Migration Process” earlier in this chapter.

For instructions and code samples to assist you in customizing the .inf files used by 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 large 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.
- Encrypted 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

Encrypted 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 (because 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.

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), which is used to migrate to the Microsoft® Windows® 2000 Active Directory® directory service, addresses issues that USMT does not handle. This tool can help you 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.

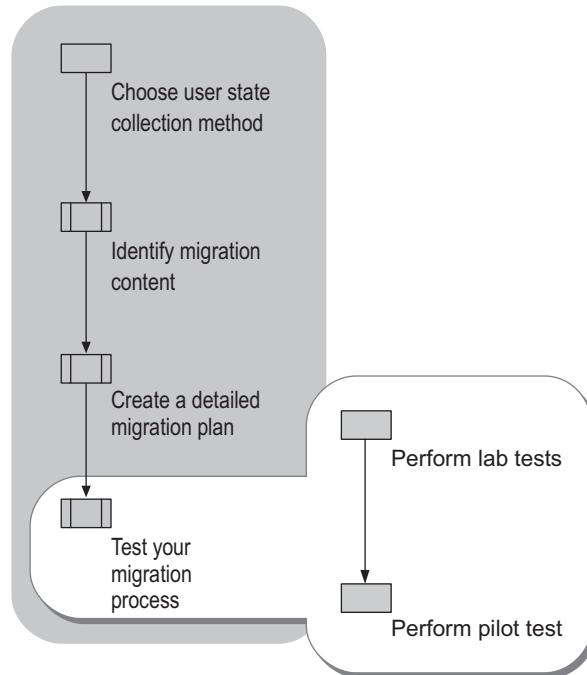
**Preparing users for changes to the desktop** The more closely that the users' new environment mirrors their previous one, the less support they will need, and the sooner they can resume productivity. If the migration involves changes to the desktop, prepare the users for these changes.

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).

# 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 5.5 shows the tasks in the testing process.

**Figure 5.5 Testing Your Migration Process**



Even with thorough testing before the migration, you can often 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 this book for information about using Remote Installation Services (RIS).
- For information about scripting in a Windows Server 2003 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>.
- 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 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 ADMT is used to migrate to Windows 2000 Active Directory, 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>.



# Glossary

## Symbols

**\$\$Rename.txt** A file that lists all files contained in a particular folder that need to be renamed from an 8.3 format name to a long file name during Setup. All file names must be in 8.3 format if you run Setup using Winnt.exe, or if you copy a set of files from one computer to another using MS-DOS.

**%windir%** The default directory where Windows is installed, most commonly C:\Windows.

**.cab file** Cabinet file. A single cabinet file that stores multiple compressed files. These files are commonly used in software installation and to reduce the file size and the associated download time for Web content.

**8.3** The standard format for file names in MS-DOS and Windows 3.1. A file name with eight or fewer characters, followed by a period (dot), followed by a three-character file name extension.

---

## 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).

**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).

**ACE** See definition for access control entry (ACE).

**ACPI** See definition for Advanced Configuration and Power Interface (ACPI).

**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.

**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.

**ADSI** See definition for Active Directory Service Interfaces (ADSI).

**Advanced Configuration and Power Interface (ACPI)** An open industry specification that defines power management on a wide range of mobile, desktop, and server computers and peripherals. ACPI is the foundation for the OnNow industry initiative that allows system manufacturers to deliver computers that start at the touch of a keyboard. ACPI design is essential to take full advantage of power management and Plug and Play. See also Plug and Play.

**answer file** A text file used to automate Setup or other installation processes. Using this text file, you can provide custom answers to Setup-related questions. Typically, you must point the Setup program to use the answer file at the same time Setup is started. Answer files can only be used on applications and operating systems that support them.

**APIC** Advanced Programmable Interrupt Controller. A distributed set of devices that form an interrupt controller.

**asynchronous** Not dependent on timing. Each application or command runs in the specified order, but the specified item does not wait for any previously started processes to finish before an application or command runs.

**attach** Run the Setup program for an application that is already staged on the destination computer. See also destination computer; detach; stage.

---

## B

**basic input/output system (BIOS)** On x86-based computers, the set of essential software routines that test hardware at startup, start the operating system, and support the transfer of data among hardware devices. The BIOS is stored in read-only memory (ROM) so that it can be executed when you turn on the computer. Although critical to performance, the BIOS is usually invisible to computer users. See also Extensible Firmware Interface (EFI).

**BINLSVC** See definition for Boot Information Negotiation Layer service (BINLSVC).

**BIOS** See definition for basic input/output system (BIOS).

**Boot Information Negotiation Layer service (BINLSVC)** A service that runs on a Remote Installation Services (RIS) server that acts on client boot requests. The display name of BINLSVC is *Remote Installation*. See also Remote Installation Services (RIS).

**bottleneck** A condition, usually involving a hardware resource, that causes a computer to perform poorly.

---

## C

**CardBus** A 32-bit PC Card.

**CD boot** Starting a computer from the retail product CD-ROM and then installing Windows on the hard disk using the Setup program on the CD. This method is much slower than installing Windows from a network and is not recommended. For an unattended Setup using the CD boot method, the Unattend.txt file must be named *Winnt.sif*. The user can select in the *winnt.sif* if they want to select the partition manually or have it automatically selected.

**Cluster service** The essential software component that controls all aspects of server cluster operation and manages the cluster database. Each node in a server cluster runs one instance of the Cluster service.

**Cmdlines.txt** A text file that GUI-mode Setup executes when installing optional components, such as applications.

---

## D

**destination computer** The computer on which you preinstall Windows that will be distributed to customers. You can either run Setup on the destination computer or copy a master installation onto a destination computer.

**detach** Remove uninstalled application files from a destination computer. See also attach; destination computer; stage.

**device ID** A unique ASCII string for the device created by enumerators to identify a hardware device and used to cross-reference data about the device stored in the registry. Distinguishes each logical device and bus from all others on the system.

**distribution share** A network folder that contains the source files for Windows products that you install. It may also contain additional device drivers and application files. This folder can be created manually or by using Setup Manager.

**Dynamic Host Configuration Protocol (DHCP)** An industry standard method for simplified and dynamic configuration of IP addresses for computers on TCP/IP networks.

---

## E

**EFI** See definition for Extensible Firmware Interface (EFI).

**Extensible Firmware Interface (EFI)** In computers with the Intel Itanium processor, the interface between a computer's firmware, hardware, and the operating system. EFI defines a new partition style called GUID partition table (GPT). EFI serves the same purpose for Itanium-based computers as the basic input/output system (BIOS) found in x86-based computers. However, it has expanded capabilities that provide a consistent way to start any compatible operating system and an easy way to add EFI drivers for new bootable devices without the need to update the computer's firmware. See also basic input/output system (BIOS).



## F

**factory mode** A mode of running Sysprep that postpones Windows Welcome or Mini-Setup and allows you to install additional drivers and applications and test the Windows installation. To run Sysprep in factory mode, use the command line **Sysprep -factory**.

**file copy** The first of the three stages of Setup, where the Windows program files and any additional files specified are copied to the computer's hard disk.

**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*.

## G

**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.

**GUI-mode Setup** The third of the three stages of Setup, during which the computers hardware and network settings are configured, you are prompted to provide an Administrator password, and you can personalize the installation.

## H-K

**HAL** See definition for hardware abstraction layer (HAL).

**hardware abstraction layer (HAL)** A thin layer of software provided by the hardware manufacturer that hides, or abstracts, hardware differences from higher layers of the operating system. By means of the filter provided by the HAL, different types of hardware look alike to the rest of the operating system. This enables the operating system to be portable from one hardware platform to another. The HAL also provides routines that enable a single device driver to support the same device on all platforms.

## L

**LAN** See definition for local area network (LAN).

**legacy** Any feature in the computer system based on older technology for which compatibility continues to be maintained in other system components.

**load balancing** A technique that is used to scale the performance of a server-based program (such as a Web server) by distributing its client requests across multiple servers within a cluster.

**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.

**long file name** A folder or file name longer than the 8.3 file name standard (up to eight characters followed by a period and an extension of up to three characters). Most versions of Windows, including Windows XP, Windows 2000, Window NT, Windows 95, and Windows 98 support long file names up to 255 characters.

## M-O

**mass-storage controller** A device on which mass-storage devices rely for access to a computer subsystem. For example, a SCSI card or IDE functionality on the motherboard is a mass-storage controller; the physical hard drive is a mass-storage device.

**master computer** A fully-assembled computer containing a master installation. See also master installation.

**master installation** A customized installation of Windows that you duplicate onto one or more destination computers.

**Message Queuing** A message queuing and routing system for Windows that enables distributed applications running at different times to communicate across heterogeneous networks and with computers that may be offline. Message Queuing provides guaranteed message delivery, efficient routing, security, and priority-based messaging. Formerly known as *MSMQ*.

**Mini-Setup** A subset of GUI-mode Setup, Mini-Setup is the first-run experience on the Windows Server 2003 family. Mini-Setup prompts for user-specific information, detects new hardware, and regenerates system IDs.

**NTLM** A security package that provides authentication between clients and servers.

---

## P-Q

**Plug and Play** A set of specifications developed by Intel Corporation that enables a computer to detect and configure a device automatically and install the appropriate device drivers.

**Preboot Execution Environment** DHCP-based remote boot technology used to boot or install an operating system on a client computer from a remote server. A RIS Server is an example of a PXE Server.

**PXE** See definition for Preboot Execution Environment.

**PXE protocol** An extension to the DHCP protocol that enables information to be sent to network-bootable systems and enables these systems to find RIS servers.

**quiet mode** Running a command-line application so that it does not display confirmation messages or any other user interface items that normally appear on screen. The switch for quiet mode is typically */q*.

---

## R

**RAID** See definition for Redundant Array of Independent Disks (RAID).

**Redundant Array of Independent Disks (RAID)** A method used to standardize and categorize fault-tolerant disk systems. RAID levels provide various mixes of performance, reliability, and cost. Some servers provide three of the RAID levels: Level 0 (striping), Level 1 (mirroring), and Level 5 (RAID-5).

**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.

**Remote Installation Services (RIS)** Software services that allow an administrator to set up new client computers remotely, without having to visit each client. The target clients must support remote booting. See also Single Instance Store (SIS).

**reseat** To prepare the operating system for delivery to the customer by clearing the event log, resetting the time clock for Windows Product Activation, and configuring the first-run experience to run the next time Windows starts. Run **Sysprep -reseat** as the final step in your manufacturing process.

**RIS** See definition for Remote Installation Server (RIS).

**Run as** A feature that provides users with a secondary logon capability. By using **Run as**, users can run applications or commands in a different security context without having to log off. **Run as** prompts the user for different credentials before running the application or command.

## S

**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.

**Server Message Block (SMB)** A file-sharing protocol designed to allow networked computers to transparently access files that reside on remote systems over a variety of networks. The SMB protocol defines a series of commands that pass information between computers. SMB uses four message types: session control, file, printer, and message.

**Setup Manager** A utility for creating and modifying answer files and configuration sets.

**Setupcl.exe** An executable program invoked by Sysprep.exe that recognizes security IDs (SIDs). It must reside in the same folder as Sysprep.exe. See also security ID (SID); Sysprep.exe.

**SID** See definition for security ID (SID).

**Single Instance Store (SIS)** A component that saves disk space on the server by maintaining a single physical copy of all identical files found. If SIS finds a duplicate file on the server, it copies the original file into the SIS store and leaves a link where the original resided. This technology is used only with Remote Installation Services. See also Remote Installation Services (RIS).

**SMB** See definition for Server Message Block (SMB).

**SMS** See definition for Systems Management Server (SMS).

**stage** Copy the directories and files to be installed to a destination computer, but do not configure any registry settings. See also attach; destination computer; detach.

**standalone server** A computer that runs Windows 2000 Server but does not participate in a domain. A standalone server has only its own database of end users, and it processes logon requests by itself. It does not share account information with any other computer and cannot provide access to domain accounts.

**synchronous** Each application or command runs in the order listed, and each item must finish before the next command is run.

**Sysprep** A tool that prepares the hard disk on a source computer for duplication to destination computers and then runs a non-Microsoft disk-imaging process. This automated installation method is used when the hard disk on the master computer is identical to those of the target computers. See also destination computer; security ID (SID).

**Sysprep.exe**

The System Preparation utility that uses the Sysprep.inf answer file to prepare a system disk image for duplication.

**Sysprep.inf** An optional answer file used by Sysprep that automates Mini-Setup and further customizes the installed operating system.

**systemroot** The path and folder name where the Windows system files are located. Typically, this is C:\Windows, although you can designate a different drive or folder when you install Windows. You can use the value %systemroot% to replace the actual location of the folder that contains the Windows system files. To identify your systemroot folder, click **Start**, click **Run**, type %systemroot%, and then click **OK**.

**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.

## T

**Terminal Services** The underlying technology that enables Remote Desktop, Remote Assistance, and Terminal Server.

**text-mode Setup** The second of the three stages of Setup, where the basic hardware of the computer (CPU, motherboard, hard disk controllers, file systems, and memory) is determined, the base operating system necessary to continue is installed, and specified folders are created.

## U-V

**Unattend.txt** The generic name for the Windows Setup answer file. In the CD boot installation method, Unattend.txt must be named Winnt.sif. See also CD boot; Windows Setup; Winnt.exe.

**unattended Setup** An automated, hands-free method of installing Windows. During installation, unattended Setup uses an answer file to supply data to Setup instead of requiring that an administrator or end user interactively provide the answers.

---

## W-Z

**WAN** See definition for wide area network (WAN).

**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).

**Winbom.ini** An .ini file that provides a bill-of-materials to incorporate into the Windows installation. Winbom.ini can control different points of the installation and configuration process: for example, it can control Sysprep during Factory mode, Windows preinstallation when starting from the Windows Preinstallation Environment (WinPE), or Windows XP configuration during Windows Welcome.

**Windows PE** See definition for Windows Preinstallation Environment (Windows PE).

**Windows Preinstallation Environment (Windows PE)** A minimal Win32 operating system with limited services, built on the Windows XP Professional kernel. Windows PE is used only in the preinstallation and deployment of Windows.

**Windows Product Activation (WPA)** A technology that reduces software piracy by requiring that each installation of a Windows product be activated with Microsoft, either through the Internet or by telephone. A unique product key is required for each installation of Windows, but Microsoft does not request or collect any information other than the Product Key during the installation. The end user may reinstall Windows using the same Product Key on the same computer as many times as necessary, but it cannot be used to install Windows on another computer. The end user can make incremental hardware upgrades to the computer. However, if the hardware is significantly altered, the end user will be required to reactivate the installation of Windows.

**Windows Setup** The program that installs the Windows operating system.

**Winnt.exe** A command-line utility used to start an unattended setup from computers running MS-DOS, Windows 3.1, or Windows for Workgroups.

**Winnt.sif** The answer file that contains information used by Setup when you install Windows using the CD boot method. See also CD boot.

**Winnt32.exe** A command-line utility used to start an unattended setup from computers running Windows 95, Windows 98, Windows NT, Windows 2000, or Windows XP.

# Index

---

## Special Characters

\$\$ subfolder 41  
\$\$Rename.txt 43–44  
\$1 subfolder 42  
\$OEM\$ 41

---

## A

Access Control Lists (ACLs) 314  
Active Directory  
    choosing automated installation methods 17  
    choosing locations for RIS servers 273–274  
    defining prestaging details 275–276  
    defining security groups 274  
    designing infrastructure 273–276  
    designing support 274–276  
    planning RIS installations 191–192  
Active Directory Migration Tool (ADMT) 316–317  
Active Directory Users and Computers Extension for RIS (Dsa.msc) 170  
additional resources  
    choosing automated installation methods 18  
    image-based installations 158–160  
    migrating user state 321  
    RIS (Remote Installation Services) 291–293  
    unattended installations 87–89  
ADMT (Active Directory Migration Tool) 316–317  
answer file-based installations  
    See also Risetup.exe; unattended installations  
    domain controllers 12  
    overview 4  
    server computers 11  
answer files  
    configuring permissions 286  
    configuring settings for Dynamic Update 54  
    creating 72, 77–79  
    defining RIS server configuration parameters 267  
    designing settings for unattended installations 55–57

answer files *(continued)*  
    GuiRunOnce See GuiRunOnce  
    identifying settings 60–62  
    overview 22  
Application Compatibility Toolkit 27, 105  
application compatibility, choosing automated installation methods 12  
assessing  
    delegation of RIS administrative tasks 213  
    master computer requirements 198–200  
    network infrastructure 200–204  
    RIS server authorization security 211–212  
    RIS server placement 192–195  
    RIS server software requirements 191–192  
    security benefits of controlling user interaction levels 209  
    security benefits of restricting client installation options 208–209  
    security for non-prestaged clients 206–207  
    security for RIS administrative tasks 214  
    security of PXE environments 205  
associating user states with computers 305  
auditing  
    existing clients 180–185  
    tasks on master installations 148–149  
authentication levels 206  
authorization locations 211  
authorization methods 212  
authorization security 211–212  
authorizers 211  
automated installations  
    boot configurations 244  
    choosing clients 242  
    choosing methods See choosing automated installation methods  
    design background 238–240  
    design tasks 241–244  
    designing post-installation tasks 63–67

- automated installations (*continued*)
  - designing tasks 58–62
  - Group Policy configurations 243–244
  - identifying post-installation tasks 63–64
  - identifying tasks 58–59
  - operating system images 241–242
  - overview 4–7
  - renaming files 238
  - RIS (Remote Installation Services) 238–244
  - Startrom.n12 239
  - startup files 244
  - tools 5–7
  - USMT (User State Migration Tool) 9
- Automatic Setup option 252
- automating tasks
  - after Mini-Setup 138–141
  - before Mini-Setup 128–133
  - design overview 126–127
  - during Mini-Setup 133–138
- automating Windows XP image installations 306

---

## B

- Binlsvc 165
- boot configurations 244
- bottlenecks 196
- building
  - master distribution share installations 287
  - master installations 143–147

---

## C

- Caution screen 248
- centralized automation 304–306
- Certificate Services 12
- Choice.osc 247
- choosing
  - Active Directory locations for RIS servers 273–274
  - automated installation methods See choosing automated installation methods
  - clients for automated installations 242
  - delegation of RIS administrative tasks 268
  - disk-imaging programs 116–117
  - distribution methods 33–34

- choosing (*continued*)
  - image distribution methods 117–121
  - methods for automating post-installation tasks 64
  - removal of RIS tools 268
  - Risetup images to host on servers 268
  - startup media 74–75, 154–155
  - Sysprep settings 149–152
  - user state collection methods 300–306
  - Winnt.exe parameters 68–69
  - Winnt32.exe parameters 69–72
- choosing automated installation methods
  - Active Directory 17
  - additional resources 18
  - application considerations 12
  - Certificate Services 12
  - clean installations 7–9
  - client computers 11
  - Cluster services 12
  - DHCP (Dynamic Host Configuration Protocol) 14
  - directory services considerations 16–17
  - domain controllers 12, 17
  - HAL (hardware abstraction layer) 15
  - hardware considerations 13, 15
  - IIS (Internet Information Services) 12
  - IP addresses 14
  - mass storage controllers 15
  - network considerations 13–14
  - operating system considerations 11
  - overview 1–7
  - post-installation tasks 64
  - processes 3–4
  - PXE (Pre-Boot eXecution Environment) 15
  - server considerations 11, 12
  - software considerations 10–12
  - testing application installation compatibility 12
  - upgrading 7–9
- CIW (Client Installation Wizard)
  - Automatic Setup option 252
  - Caution screen 248
  - Choice.osc 247
  - creating configurations 289

CIW (Client Installation Wizard) *(continued)*

- Custom Setup option 252
- default configurations 246
- default screens 246
- defining configurations 253–258
- defining modifications to screens 256–257
- defining multilanguage processes 258
- defining new screens 254–256
- defining OSC variables 254–256
- defining screens to remove 257
- design background 245–249
- design process overview 245
- design tasks 249–258
- Dupauto.osc 247
- Error screen 247
- Install.osc 248
- Login.osc 247
- Logon screen 247
- Operating System Choice screen 248
- operating system installation options 250
- Oschoice.osc 248
- OSChooser 170
- OSCMML tags See OSCML tags
- Restart Setup option 252
- screen functions 246–249
- setup options in Group Policy 251–252
- Setup Options screen 247
- Summary screen 248
- Tools option 252
- user interaction 246
- Warning.osc 248
- Welcome screen 246–247
- Welcome.osc 246–247

## clean installations

- choosing automated installation methods 7–9
- compared to upgrading 28–33
- image-based installations 95
- MS-DOS startup disks 84
- unattended installations 83–85

## cleanup tasks on master installations 148–149

## client computers 11

Client Installation Wizard See CIW (Client Installation Wizard)

## Cluster services 12

## Cmdlines.txt

- automating post-installation tasks 64
- configuring to perform tasks 65–66
- creating commands 230
- described 23, 96
- designing automated setup tasks 126
- Rissetup image design considerations 229–230

## comparing

- clean installations and upgrades 28–33
- disk image distribution methods 120–121

## compatibility

- HAL (hardware abstraction layer) 15
- hardware and software 26, 105, 181
- testing application installations for image-based installations 12

## configuration tasks on master installations 148–149

## configuring

- answer file permissions 286
- answer file settings for Dynamic Update 54
- Cmdlines.txt to perform tasks 65–66
- disk settings on master installations 143
- disk settings on unattended installations 48–49
- domain controller support for RIS 280
- GuiRunOnce to perform tasks 66–67
- image folder permissions 286
- master computer operating systems 284–285
- master installations 144–147, 283–286
- networking support for RIS 280
- production clients for RIS 281–282
- referral servers 288
- RIS (Remote Installation Services) 278
- RIS servers 287–288
- shared folders for Dynamic Update files 53
- Winnt32.exe settings for Dynamic Update 54

## converting short file names to long file names 43–44

## counters 197

## creating

- answer files 72, 77–79
- CIW configurations 289
- Cmdlines.txt commands 230
- disk configuration plans for image-based installations 124–125
- disk configuration plans for unattended installations 48–49
- disk images 141–152
- distribution shares 72, 80–81
- GuiRunOnce commands 232–233
- migration plans 311–318
- MS-DOS boot disks 77, 156
- network boot disks 76, 156
- production RIS servers 282
- startup media for destination computers 72–77, 153–156
- TCP/IP boot disks 76, 156
- test RIS environments 279–280
- user state migration plans for image-based installations 123
- user state migration plans for unattended installations 47

## custom installations 5

## Custom Setup option 252

---

**D**

## data encryption 314

## definitions

- image-based installations 95–96
- unattended installations 23–24

## deploying

- images 157
- operating systems 290–291
- RIS (Remote Installation Services) 162–172, 278

## designing

- Active Directory infrastructure 273–276
- Active Directory support 274–276
- answer file settings for unattended installations 55–57
- automated installation tasks 58–62
- automated post-installation tasks 63–67

designing (*continued*)

- automated setup tasks See designing automated setup tasks
- CIW process overview 245
- distribution processes 39–45
- distribution shares 39–44
- image delivery processes 114–121
- image-based installations See designing image-based installations with Sysprep
- media distribution processes 44–45
- optimal security configurations with prestaged clients 271
- preinstallation tasks for image-based installations 121–125
- preinstallation tasks for unattended installations 45–55
- Riprep-based installations 216
- RIS deployment modes 234
- RIS installations See designing RIS installations
- RIS network deployment configurations 260–264
- RIS server authorization methods 272–273
- RIS server configuration overview 259
- RIS server configuration tasks 260
- RIS server properties 265–267
- RIS server security 269–273
- Risetup-based installations 223
- secure RIS server responses and load balancing 269–271
- security for non-prestaged RIS clients 271
- Setup settings for unattended installations 55–57, 68–72
- test RIS environments 276–277
- unattended installations See designing unattended installations

## designing automated setup tasks

- automating tasks after Mini-Setup 138–141
- automating tasks before Mini-Setup 128–133
- automating tasks during Mini-Setup 133–138
- overview 126–127

## designing image-based installations with Sysprep

- additional resources 158–160
- creating startup media for destination computers 153–156



designing image-based installations with Sysprep  
(*continued*)

- defining disk images 106–114
- deploying images 157
- designing automated setup tasks See designing automated setup tasks
- designing image delivery processes 114–121
- designing preinstallation tasks for image-based installations 121–125
- identifying inventory requirements 97–105
- overview 91–97

designing RIS installations

See also RIS (Remote Installation Services)

- Active Directory infrastructure 273–276
- Active Directory support 274–276
- additional resources 291–293
- automated installations 238–244
- choosing Active Directory locations for servers 273–274
- choosing Risetup images to host on servers 268
- choosing to delegate administrative tasks 268
- choosing to remove tools 268
- Client Installation Wizard See CIW (Client Installation Wizard)
- defining Active Directory security groups 274
- defining answer file associations 267
- defining prestaging details 275–276
- defining server configuration parameters 267–268
- deployment mode overview 234
- deployment processes 162–172
- designing Riprep-based installations 216
- installation types 215
- interactive installations 234–237
- network deployment configurations 260–264
- optimal security configurations with prestaged clients 271
- overview 161, 215
- renaming files 238
- Riprep image design background 216–217
- Riprep image design tasks 218–223
- Riprep image designs 223

designing RIS installations (*continued*)

- Riprep user profiles 223
- Risetup image design background 224–225
- Risetup image design tasks 225–233
- Risetup-based installation designs 223
- secure server responses and load balancing 269–271
- security for non-prestaged clients 271
- server authorization methods 272–273
- server configuration overview 259
- server configuration tasks 260
- server properties 265–267
- server security 269–273
- test RIS environments 276–277

designing unattended installations

See also unattended installations

- additional resources 87–89
- choosing distribution methods 33–34
- choosing methods for automating post-installation tasks 64
- choosing startup media 74–75
- choosing Winnt.exe parameters 68–69
- choosing Winnt32.exe parameters 69–72
- clean installations vs. upgrades 28–33
- configuring Cmdlines.txt to perform tasks 65–66
- configuring GuiRunOnce to perform tasks 66–67
- creating answer files 72, 77–79
- creating distribution shares 72, 80–81
- creating startup media for destination computers 72–77
- designing answer file settings 55–57
- designing automated installation tasks 58–62
- designing automated post-installation tasks 63–67
- designing Setup settings 55–57, 68–72
- distribution processes 39–45
- distribution shares 39–44
- evaluating distribution methods 35–38
- evaluating hardware support for startup media 74
- identifying answer file settings 60–62
- identifying automated installation tasks 58–59

- designing unattended installations (*continued*)
  - identifying automated post-installation tasks 63–64
  - overview 19–20
  - preinstallation tasks 45–55
  - processes 21
  - upgrades vs. clean installations 28–33
- DHCP (Dynamic Host Configuration Protocol)
  - choosing automated installation methods 14
  - planning RIS installations 191, 193, 204
- directory services 16–17
- disk configuration plans
  - components 49
  - creating for image-based installations 124–125
  - creating for unattended installations 48–49
- disk images
  - comparing distribution methods 120–121
  - creating 141–152
  - defining 106–114
  - deploying 157
  - described 94
  - distributing across networks 118–119
  - distributing with media 119–120
  - domain controllers 113
  - EFS (Encrypting File System) 114
  - Group Policy 114
  - HAL (hardware abstraction layer) 108–110
  - hardware 106, 108–111
  - mass storage controllers 111
  - Mini-Setup 114
  - operating system considerations 106, 108, 113–114
  - Plug and Play 113
  - portable computer devices 110
  - software 106, 111–114
  - static IP addresses 114
- disk subsystem performance 196
- distributing
  - disk images across networks 118–119
  - disk images with media 119–120

- distribution methods
  - choosing for unattended installations 33–34
  - choosing image 117–121
  - comparing disk image 120–121
  - evaluating for unattended installations 35–38
- distribution shares
  - \$\$ subfolder 41
  - \$1 subfolder 42
  - \$OEM\$ 41
  - creating 72, 80–81
  - Help subfolder 42
  - i386 41
  - overview 22
  - Sysprep subfolder 42
  - System32 subfolder 42
  - Textmode subfolder 41
  - unattended installations 35–36, 39–44
- DNS (Domain Name System) 191
- domain controllers
  - choosing automated installation methods 12, 17
  - configuring support for RIS 280
  - disk images 113
  - image-based installations 95
- Domain Name System (DNS) 191
- downloading Dynamic Update files 51–52
- Dsa.msc (Active Directory Users and Computers Extension for RIS) 170
- Dupauto.osc 247
- Dynamic Host Configuration Protocol *See* DHCP (Dynamic Host Configuration Protocol)
- Dynamic Update 50–55

---

## E

- EFS (Encrypting File System) 114, 314
- Error screen 247
- evaluating
  - clean installations vs. upgrades 32–33
  - costs vs. benefits of migrating settings 310
  - creation of UUIDs 185
  - disk image operating system differences 108
  - distribution methods for unattended installations 35–38

*evaluating (continued)*

- hardware differences for disk images 108–111
- hardware for unattended installations 24–28
- hardware support for startup media 74, 154
- network installation points 202–203
- NTLM authentication levels 206
- operating system configurations 187–189
- operating system settings for disk images 113–114
- remote boot capabilities of RIS clients 177–179
- RIS client hardware 174–175
- RIS client prestaging processes 185–186
- RIS server hardware 190
- RIS server requirements 190–197
- security for operating system images 210
- software differences for disk images 111–114
- software for unattended installations 24–28
- unattended installation upgrade paths 30–31

**F**

- Factory mode 95, 128–133
- file-copy mode 24
- Files and Settings Transfer Wizard
  - image-based installations 123
  - migrating user state 298, 314
  - RIS installations 184
  - unattended installations 47
- forwarding client DHCP requests through routers 204
- fully-automated installations *See* automated installations

**G**

- Group Policy
  - automated installations 243–244
  - CIW (Client Installation Wizard) 251–252
  - disk images 114
  - interactive installations 237
- GUI mode 24
- GuiRunOnce
  - automating post-installation tasks 64
  - automating tasks after Mini-Setup 138–141

*GuiRunOnce (continued)*

- configuring to perform tasks 66–67
- creating commands 232–233
- described 23, 96
- Risetup image design considerations 231–233

**H**

- HAL (hardware abstraction layer)
  - choosing automated installation methods 15
  - disk images 108–110
  - image-based installations 95, 99–101
  - RIS installations 175–176
- hardware
  - choosing automated installation methods 13, 15
  - compatibility 26, 181
  - configurations and Risetup images 227–228
  - configurations and separate Riprep images 220–221
  - disk images 106, 108–111
  - evaluating RIS clients 174–175
  - evaluating RIS servers 190
  - evaluating support for startup media 74, 154
  - image-based installations 99–103, 105
  - master computer requirements 198
  - RIS installations 181–182
  - unattended installations 24–28
- hardware abstraction layer *See* HAL (hardware abstraction layer)
- Hardware Compatibility List 175
- Help subfolder 42

**I**

- i386 41
- identifying
  - answer file settings 60–62
  - auditing tasks on master installations 148–149
  - automated installation tasks 58–59
  - automated installation tasks to perform after Mini-Setup 139
  - automated installation tasks to perform before Mini-Setup 130–131

identifying (*continued*)

- automated installation tasks to perform during Mini-Setup 134–136
- automated post-installation tasks 63–64
- cleanup tasks on master installations 148–149
- configuration file settings for Sysprep.inf 137–138
- configuration file settings for Winbom.ini 132
- configuration file settings to use after Mini-Setup 141
- configuration files to use after Mini-Setup 140
- configuration files to use before Mini-Setup 132
- configuration files to use during Mini-Setup 136–137
- configuration tasks on master installations 148–149
- Dynamic Update files 51–52
- inventory requirements for image-based installations 97–105
- migration content 307–310
- RIS client requirements 174
- security concerns 314–315
- settings for user productivity 309
- startup media to use for image-based installations 155
- user data to migrate 308
- user settings to migrate 309–310

## IIS (Internet Information Services) 12

## image delivery

- choosing disk-imaging programs 116–117
- choosing image distribution methods 117–121
- comparing disk image distribution methods 120–121
- designing processes 114–121
- distributing disk images across networks 118–119
- distributing disk images with media 119–120
- long file names 116
- NTFS 3.1 116
- overview 114

## image distribution 117–121

## image-based installations

- See *also* Riprep.exe; Sysprep
- additional resources 158–160

image-based installations (*continued*)

- Application Compatibility Toolkit 105
- background information 94–97
- choosing automated installation methods 15
- choosing disk-imaging programs 116–117
- choosing image distribution methods 117–121
- clean installations 95
- client computers 11
- creating disk configuration plans 124–125
- creating startup media for destination computers 153–156
- creating user state migration plans 123
- definitions 95–96
- deploying images 157
- designing automated setup tasks See designing automated setup tasks
- designing image delivery processes 114–121
- designing preinstallation tasks 121–125
- designing with Sysprep 91
- disk images See disk images
- domain controllers 12, 95
- HAL (hardware abstraction layer) 15, 95, 99–101
- hardware considerations 99–103, 105
- identifying inventory requirements 97–105
- identifying which startup media to use 155
- long file names 116
- mass storage controllers 101
- master installations See master installations
- NTFS 3.1 116
- overview 4, 92
- portable computer devices 102
- processes 93
- requirements 95
- software considerations 103–105
- terms 95–96
- testing application installation compatibility 12
- Upgrade Advisor 105
- Windows Catalog 105
- Windows PE (Windows Preinstallation Environment) 125

## Install.osc 248

---

**installations**

- answer file-based See answer file-based installations
- automated See automated installations
- clean See clean installations
- image-based See image-based installations
- interactive 234–237
- master See master installations
- Riprep-based 216–223
- RIS (Remote Installation Services) See designing RIS installations
- Risetup-based See Risetup.exe
- Sysprep, using See Sysprep
- unattended See unattended installations

**installing**

- master computer operating systems 283–284
- master installations 144–147
- interactive installations 234–237
- Internet Information Services (IIS) 12
- inventory requirements, identifying for image-based installations 97–105
- IP addresses
  - choosing automated installation methods 14
  - static 114

---

**L**

- lab testing 320
- language support 258
- load balancing 194, 269
- Login.osc 247
- Logon screen 247
- long file names 43–44, 116

---

**M**

- manual migration 302–304
- mass storage controllers
  - choosing automated installation methods 15
  - disk images 111
  - image-based installations 101
- master installations
  - building 143–147
  - configuring 144–147, 283–286

**master installations (continued)**

- configuring disk settings 143
- creating disk images 152
- described 94
- identifying cleanup, configuration, and auditing tasks 148–149
- installing 144–147
- preparing by running Sysprep 148–152
- reusing 222–223
- software configurations 218–219
- media distribution 37–38, 44–45, 117, 119–121
- memory performance 196
- Microsoft Download Center 51
- Microsoft Windows Preinstallation Environment (Windows PE) 49, 125
- migrating user state
  - adapting plans for domain migration 316–317
  - additional resources 321
  - ADMT (Active Directory Migration Tool) 316–317
  - centralized automation 304–306
  - choosing user state collection methods 300–306
  - creating plans for image-based installations 123
  - creating plans for migration 311–318
  - creating plans for unattended installations 47
  - data issues 312–313
  - educating users 318
  - evaluating costs vs. benefits of migrating settings 310
  - file relocation issues 313
  - identifying migration content 307–310
  - identifying security concerns 314–315
  - identifying settings for user productivity 309
  - identifying user data to migrate 308
  - identifying user settings to migrate 309–310
  - managing data encryption during migration 314
  - manual migration 302–304
  - overview 295–296
  - parallel deployments 304
  - preparing files and folders for migration 318
  - processes 297–300
  - relocating registry entries 315–316
  - restoring lost ACLs 314

- migrating user state *(continued)*
  - RIS installations 183–184
  - scheduling migrations 317
  - scripted-manual migrations 303–304
  - securing user state during migration 315
  - storage issues 312–313
  - testing migration processes 319–320
  - tools 297–300
  - translating registry entries 315–316
  - user-driven migrations 306
  - Windows XP registry restrictions 316
  - wipe-and-load deployments 303

- Mini-Setup
  - automating tasks after 138–141
  - automating tasks before 128–133
  - automating tasks during 133–138
  - described 23, 95
  - disk images 114

- MS-DOS boot disks 77, 156
- MS-DOS disk configuration tools 48
- MS-DOS startup disks 84
- multiple language support 258

---

## N

- network distribution 117–121
- Network Load Balancing (NLB) 11
- networks
  - assessing infrastructure 200–204
  - boot disks 76, 156
  - boot from PXE-enabled clients 290–291
  - choosing automated installation methods 13–14
  - designing RIS deployment configurations 260–264
  - distribution 117–121
  - evaluating installation points 202–203
  - planning RIS installations 195, 200–204
  - security enhancement planning 207
- NLB (Network Load Balancing) 11
- NTFS 3.1 116
- NTLM authentication levels 206

## O

- Operating System Choice screen 248
- Oschoice.osc 248
- OSChooser 170
- OSCML tags
  - CIW error screens 249
  - defining CIW configurations 253
  - defining modifications to CIW screens 256
  - defining new CIW screens 254–255
  - defining OSC variables 254–255
  - defining screens to remove 257

---

## P

- parallel deployments 304
- performance 195–197
- pilot testing 320
- planning
  - Dynamic Update for unattended installations 50–55
  - network security enhancements 207
  - RIS installations *See* planning RIS installations
  - RIS network security *See* planning RIS network security
  - RIS server performance 195–197
  - security for RIS administrative tasks 212–214
- planning RIS installations
  - Active Directory 191–192
  - assessing master computer requirements 198–200
  - assessing network infrastructure 200–204
  - assessing RIS server placement 192–195
  - assessing server software requirements 191–192
  - auditing existing clients 180–185
  - client computers UUIDs 184
  - DHCP (Dynamic Host Configuration Protocol) 191, 193, 204
  - DNS (Domain Name System) 191
  - evaluating creation of UUIDs 185
  - evaluating network installation points 202–203
  - evaluating operating system configurations 187–189

planning RIS installations (*continued*)

- evaluating remote boot capabilities of RIS clients 177–179
- evaluating RIS client hardware 174–175
- evaluating RIS client prestaging processes 185–186
- evaluating RIS server hardware 190
- evaluating RIS server requirements 190–197
- forwarding client DHCP requests through routers 204
- hardware 181–182
- Hardware Compatibility List 175
- identifying client requirements 174
- inventories 180–183
- load balancing 194
- migrating user state 183–184
- network load considerations 195
- overview 172–173
- planning RIS network security See planning RIS network security
- redirecting RIS client requests 203
- RIS client HAL types 175–176
- server performance 195–197
- software 181–183
- Windows XP Professional Upgrade Center 175

planning RIS network security

- assessing delegation of RIS administrative tasks 213
- assessing security benefits of controlling user interaction levels 209
- assessing security benefits of restricting client installation options 208–209
- assessing security for non-prestaged clients 206–207
- assessing security for RIS administrative tasks 214
- assessing security of PXE environments 205
- assessing server authorization security 211–212
- evaluating NTLM authentication levels 206
- evaluating security for operating system images 210
- network security enhancements 207

planning RIS network security (*continued*)

- overview 204
- planning security for RIS administrative tasks 212–214

Plug and Play 113

Policy See Group Policy

portable computer devices

- disk images 110
- image-based installations 102

Pre-Boot eXecution Environment (PXE) 15, 169, 205

preparing

- Dynamic Update files 52–53
- files and folders for migration 318
- master installations by running Sysprep 148–152

prestaging computer accounts 185–186, 275–276

processor performance 196

PXE (Pre-Boot eXecution Environment) 15, 169, 205

## R

Rbfg.exe (Remote Boot Floppy Generator) 170

redirecting RIS client requests 203

referral servers 288

relocating

- files during migration 313
- registry entries during migration 315–316

remote boot capabilities of RIS clients 177–179

Remote Boot Floppy Generator (Rbfg.exe) 170

Remote Installation Preparation Wizard See Riprep.exe

Remote Installation Services See RIS (Remote Installation Services)

Remote Installation Services Setup See Risetup.exe

renaming files 238

replicating images 286

Restart Setup option 252

restoring

- lost ACLs 314
- user states 306

Riprep.exe

- designing installations 216
- hardware configurations and separate Riprep images 220–221
- image design background 216–217

*Riprep.exe (continued)*

- image design tasks 218–223
- image designs 223
- master operating system image requirements 199
- operating system images 218
- operating system settings 221–222
- overview 6, 170
- reusing master installations and WPA 222–223
- running on master computers 286
- software application configurations and separate images 220
- software configurations for master installations 218–219
- software settings 221–222
- testing images and user profiles 285
- user profiles 223

*RIS (Remote Installation Services)*

- Active Directory Users and Computers Extension for RIS (Dsa.msc) 170
- additional resources 291–293
- authorization locations 211
- authorization methods 212
- authorizers 211
- Binlsvc 165
- boot floppy disks 291
- building master distribution share installations 287
- choosing Active Directory locations for servers 273–274
- choosing Risetup images to host on servers 268
- choosing to delegate administrative tasks 268
- choosing to remove tools 268
- Client Installation Wizard *See* CIW (Client Installation Wizard)
- components 165–166, 169–170
- configuring 278
- configuring answer file permissions 286
- configuring domain controller support 280
- configuring image folder permissions 286
- configuring master computer operating systems 284–285
- configuring master installations 283–286

*RIS (Remote Installation Services) (continued)*

- configuring networking support 280
- configuring production clients 281–282
- configuring servers 287–288
- creating production servers 282
- creating test environments 279–280
- defining Active Directory security groups 274
- defining answer file associations 267
- defining distribution of server images 264
- defining number of servers 262
- defining prestaging details 275–276
- defining server configuration parameters 267–268
- defining server placements 263
- deploying 278
- deploying operating systems 290–291
- deployment processes 162–172
- deployment teams 164
- designing Active Directory infrastructure 273–276
- designing Active Directory support 274–276
- designing network deployment configurations 260–264
- designing optimal security configurations with prestaged clients 271
- designing secure server responses and load balancing 269–271
- designing security for non-prestaged clients 271
- designing server authorization methods 272–273
- designing server properties 265–267
- designing server security 269–273
- designing test environments 276–277
- evaluating client hardware 174–175
- evaluating server hardware 190
- installation setup processes 167–168
- installations *See* designing RIS installations
- installing master computer operating systems 283–284
- limitations 171–172
- network infrastructure configuration 280–281
- new capabilities 164–165
- OSChooser 170



RIS (Remote Installation Services) *(continued)*

- overview 5, 164
- planning installations See planning RIS installations
- PXE specifications 169
- Rbfg.exe (Remote Boot Floppy Generator) 170
- referral server configurations 288
- remote boot processes 167–168
- replicating images to other servers 286
- Riprep.exe See Riprep.exe
- Risetup.exe See Risetup.exe
- server configuration design overview 259
- server configuration design tasks 260
- SIS service 166
- tasks 171
- TFTPD (Trivial File Transfer Protocol Daemon) 166

Risetup.exe

- Cmdlines.txt 229–230
- designing installations 223
- GuiRunOnce 231–233
- hardware configurations and Risetup images 227–228
- image design background 224–225
- image design tasks 225–233
- installing applications and drivers 229–233
- operating system images 225
- operating system settings 233
- overview 6, 169
- software configurations and Risetup images 226–227

Run as command 214

running Sysprep 149–152

## S

scheduling migrations 317

scripted-manual migrations 303–304

security

- authorization 211–212
- defining Active Directory security groups 274
- designing for non-prestaged RIS clients 271
- designing optimal configurations with prestaged clients 271

security *(continued)*

- designing RIS server 269–273
- designing RIS server authorization methods 272–273
- designing secure RIS server responses and load balancing 269–271
- migrating user state 314–315
- planning RIS networks See planning RIS network security

server computers 11–12

server farms 11

Setup

- choosing Winnt.exe parameters 68–69
- choosing Winnt32.exe parameters 69–72
- designing settings for unattended installations 55–57, 68–72

Setup Manager (Setupmgr.exe)

- creating answer files 78–79
- creating distribution shares 80
- described 23

Setup Options screen 247

Setupmgr.exe See Setup Manager (Setupmgr.exe)

short file names 43–44

SIS (Single Instance Store) service 166

software

- application configurations and separate Riprep images 220
- assessing RIS server requirements 191–192
- choosing automated installation methods 10–12
- compatibility 26, 181
- configurations and Risetup images 226–227
- configurations for master installations 218–219
- disk images 106, 111–114
- image-based installations 103–105
- Riprep settings 221–222
- RIS installations 181–183
- unattended installations 24–28

Startrom.n12 239

startup files 244

startup media

- choosing 74–75, 154–155
- creating boot disks 76–77, 156

- startup media (*continued*)
  - creating for destination computers 72–77, 153–156
  - evaluating hardware support 74, 154
  - identifying for image-based installations 155
- static IP addresses 114
- storing user states 306
- structuring distribution shares 40
- Summary screen 248
- Sysprep
  - See also image-based installations
  - choosing settings 149–152
  - definitions 95–96
  - designing image-based installations 91
  - features 96–97
  - overview 6
  - preparing master installations by running 148–152
  - running 149–152
  - terms 95–96
- Sysprep subfolder 42
- Sysprep.inf
  - automating tasks after Mini-Setup 138–141
  - automating tasks during Mini-Setup 133–138
  - described 96
  - designing automated setup tasks 126
  - identifying configuration file settings 137–138
- System Preparation Tool See Sysprep
- System32 subfolder 42

---

## T

- TCP/IP boot disks 76, 156
- terms
  - image-based installations 95–96
  - unattended installations 23–24
- test RIS environments
  - creating 279–280
  - designing 276–277
- testing
  - application installation compatibility 12
  - migration processes 319–320
  - Riprep images and user profiles 285

- text mode 24
- Textmode subfolder 41
- TFTPD (Trivial File Transfer Protocol Daemon) 166
- third-party disk configuration tools 49
- tools
  - automated installations 5–7
  - migration process 297–300
  - MS-DOS disk configuration tools 48
  - third-party disk configuration tools 49
  - Unattended Setup See unattended installations
  - User State Migration Tool See USMT (User State Migration Tool)
  - Windows 98 disk configuration tools 48
  - Winnt.exe and Winnt32.exe 7
- Tools option 252
- translating registry entries during migration 315–316
- Trivial File Transfer Protocol Daemon (TFTPD) 166

---

## U-V

- Unattend.txt 23, 127
- unattended installations
  - \$\$Rename.txt 43–44
  - additional resources 87–89
  - Application Compatibility Toolkit 27
  - clean installations 83–85
  - configuring disk settings 48–49
  - converting short file names to long file names 43–44
  - creating disk configuration plans 48–49
  - creating startup media for destination computers 72–77
  - creating user state migration plans 47
  - definitions 23–24
  - designing See designing unattended installations
  - designing media distribution processes 44–45
  - designing preinstallation tasks 45–55
  - distribution shares 35–36, 39–44
  - hardware evaluations 24–28
  - identifying supplemental device drivers 27
  - media distribution 37–38
  - overview 6–7, 20, 22–24
  - performing 81–86

- unattended installations (*continued*)
  - planning for Dynamic Update 50–55
  - software evaluations 24–28
  - terms 23–24
  - upgrading installations 86
  - upgrading operating systems 9
  - Windows Catalog 26
  - Windows PE (Windows Preinstallation Environment) 49
  - Windows Upgrade Advisor 26
- Unattended Setup See unattended installations
- universally unique identifiers See UUIDs (universally unique identifiers)
- Upgrade Advisor 105
- upgrading operating systems
  - automated installation tools 9
  - choosing automated installation methods 7–9
  - compared to clean installations 28–33
  - unattended installations 86
- user state collection methods
  - centralized automation 304–306
  - choosing 300–306
  - manual migration 302–304
  - scripted-manual migration 303–304
  - user-driven migration 306
- user state migration See migrating user state
- User State Migration Tool See USMT (User State Migration Tool)
- user-driven migration 306
- USMT (User State Migration Tool)
  - automated installations 9
  - image-based installations 123
  - migrating user state 298–300, 314
  - RIS installations 184
  - unattended installations 47
- utilities See tools
- UUIDs (universally unique identifiers)
  - client computers 184
  - evaluating creation of 185
  - prestaging computer accounts 185–186
- viewing lists of registered file types 308

## W-Z

- Warning.osc 248
- Welcome screen 246–247
- Welcome.osc 246–247
- Winbom.ini
  - automating tasks before Mini-Setup 128–133
  - described 96
  - designing automated setup tasks 127
  - identifying configuration file settings 132
- Windows 98 disk configuration tools 48
- Windows Catalog 26, 105
- Windows Network Load Balancing (NLB) 11
- Windows Preinstallation Environment (Windows PE) 49, 125
- Windows Product Activation (WPA) 222–223
- Windows Server 2003 automated installation tools 5–7
- Windows Upgrade Advisor 26, 105
- Windows XP Professional Upgrade Center 175
- Windows XP registry restrictions 316
- Windows XP Upgrade Advisor 26, 105
- Winnt.exe 7, 68–69
- Winnt.sif 23
- Winnt32.exe 7, 54, 69–72
- wipe-and-load deployments 303
- wizards
  - Client Installation Wizard See CIW (Client Installation Wizard)
  - Files and Settings Transfer Wizard See Files and Settings Transfer Wizard
  - Mini-Setup See Mini-Setup
  - OSChooser (Client Installation Wizard) 170
- WPA (Windows Product Activation) 222–223

