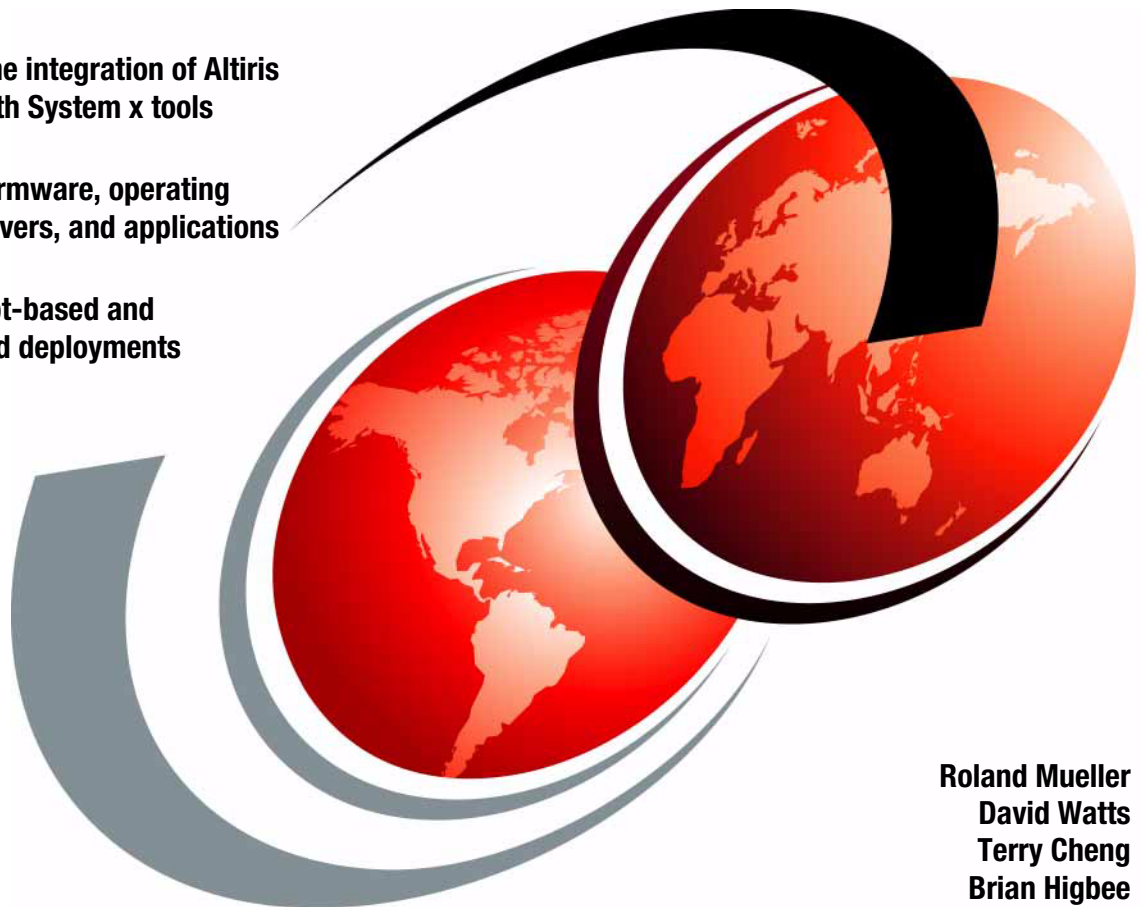


Deployment using Altiris on IBM System x and BladeCenter Servers

Describes the integration of Altiris
products with System x tools

Deploying firmware, operating
systems, drivers, and applications

Covers script-based and
image-based deployments



Roland Mueller
David Watts
Terry Cheng
Brian Higbee



International Technical Support Organization

**Deployment using Altiris on IBM System x and
BladeCenter Servers**

July 2006

Note: Before using this information and the product it supports, read the information in “Notices” on page vii.

First Edition (July 2006)

This edition applies to Altiris Deployment Solution 6.5, running on IBM System x and IBM BladeCenter servers.

© Copyright International Business Machines Corporation 2006. All rights reserved.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Notices	vii
Trademarks	viii
Preface	ix
The team that wrote this redbook	ix
Become a published author	xi
Comments welcome	xii
Chapter 1. Introduction	1
1.1 Altiris Deployment Solution	2
1.2 Comparing Deployment Solution with Deployment Server	2
1.3 Other solutions Altiris offers	4
1.3.1 Level 1	4
1.3.2 Level 2	5
1.3.3 Level 3	5
1.4 Why IBM and Altiris	6
1.5 This IBM Redbook	7
Chapter 2. Installation and configuration	9
2.1 Installing Altiris Deployment Solution 6.5	10
2.1.1 Deployment Solution components	10
2.1.2 Deployment Server system requirements	11
2.1.3 Simple installation	13
2.1.4 Custom installation	18
2.1.5 Component installation	25
2.1.6 Installing Altiris hotfixes	26
2.1.7 Applying license activation keys	27
2.2 Integrating the ServerGuide Scripting Toolkit	28
2.2.1 Installation of the ServerGuide Scripting Toolkit	29
2.2.2 Configuring the ServerGuide Scripting Toolkit source tree	35
2.3 Installation and integration of the Deployment Agent	46
2.3.1 Installing the Deployment Agent on Windows	47
2.3.2 Installing the Deployment Agent on Linux	58
2.4 Communicating with Deployment Solution	58
2.4.1 Which pre-boot operating system do you want to use?	60
2.4.2 Which automation boot method works best?	61
2.5 Configuring and using PXE pre-boot environment	64
2.5.1 Determining the number of PXE servers you need	65
2.5.2 Enabling network boot on the client computer	66

2.5.3	Connecting to the Deployment Server using PXE	67
2.5.4	Using the PXE across multiple subnets	68
2.6	Integrating with the IBM Service Processor Discovery utility	69
2.6.1	Configuring the IBM Service Processor Discovery utility	70
2.7	Best practices	75
2.7.1	Create a backup of sample jobs	75
2.7.2	Set PXE to use Ethernet port 0 rather than port 1	75
2.7.3	Change the primary lookup key to Serial Number	76
2.7.4	Synchronize the display names with NetBIOS computer name	77
Chapter 3.	Scenarios	79
3.1	Initial deployment	80
3.1.1	Configurations tab	80
3.1.2	Jobs tab	85
3.1.3	Advanced tab	88
3.2	Pre-staging computers for deployment	89
3.2.1	Pre-staging computers manually from the Deployment Console	90
3.2.2	Pre-staging computers using a CSV file	93
3.3	Linking multiple deployment jobs together	93
3.4	Job troubleshooting	96
3.5	Common issues	99
Chapter 4.	IBM hardware configuration and updating	103
4.1	System updates	104
4.1.1	Updating system BIOS	104
4.1.2	Capturing and deploying CMOS settings	106
4.1.3	Updating ServeRAID BIOS/firmware	107
4.1.4	Additional updates	109
4.1.5	Integrating with IBM UpdateXpress	113
4.2	Hardware configuration	120
4.2.1	Configuring RAID	120
4.2.2	Configuring a Fibre Channel HBA for boot from SAN	129
4.2.3	Capturing and deploying RAID configurations	134
4.2.4	Server disposal and reset RAID	135
Chapter 5.	Using script-based deployment	139
5.1	Script-based deployment versus image-based deployment	140
5.2	Script-based deployment of Windows and Linux	140
5.2.1	Integrating operating system installation media and device drivers	142
5.2.2	Preparing a Windows answer file	142
5.2.3	Creating a Windows Scripted Install job	145
5.2.4	Configuring HTTP and FTP for Linux scripted installations	150
5.2.5	Preparing a Linux kickstart file	151
5.2.6	Creating a Linux Scripted Install job	154

5.3	Deploying VMware ESX Server 2.5	157
5.3.1	Copy the installation media to the Deployment Share	157
5.3.2	Configuring HTTP and FTP for installing ESX Server 2.5	157
5.3.3	Customize a deployment job with the script and imaging tasks	161
Chapter 6. Using image-based deployment		167
6.1	Comparing with Symantec Ghost Solutions Suite	168
6.1.1	Common features	168
6.1.2	Altiris Deployment Solution	168
6.1.3	Symantec Ghost Solutions Suite	169
6.2	Image-based deployment versus Script-based deployment	169
6.3	Imaging Windows and Linux	170
6.3.1	Capturing a donor image	170
6.3.2	Deploying the image	176
6.3.3	Using multicast	182
6.4	Integrating Sysprep with Deployment Solution	193
6.4.1	Integrating the Sysprep files	194
6.4.2	Configuring Sysprep global settings	196
6.4.3	Using Sysprep during image capture	199
6.4.4	Using Sysprep during image deployment	201
6.5	Creating hardware independent Windows images	202
6.5.1	Using Microsoft Sysprep to achieve hardware independence	204
6.6	Imaging with Windows PE	220
Chapter 7. Post operating system application installation		229
7.1	Application deployment	230
7.1.1	Deploying IBM Director Agent 5.10	230
7.1.2	Deploying Microsoft SQL Server 2000 (case study)	235
7.2	Package deployment	239
7.2.1	Install a Microsoft Windows hotfix package	239
7.3	Using Wise Packager for Deployment Solution	242
7.3.1	Capturing an application installation	242
7.3.2	Guidelines for using Wise SetupCapture	247
Chapter 8. Integrating with IBM Director		249
8.1	How to integrate with IBM Director	250
8.2	Upward integration	251
8.2.1	Altiris Notification Server 6.0 with Service Pack 3	251
8.2.2	Altiris Connector Solution 6.1	262
8.2.3	Altiris Connector for IBM Director	267
8.2.4	Connector Agent for IBM Director	272
8.2.5	Final configuration	280
8.3	Integration by extension	289
8.3.1	Deployment Server Extension 1.0 for IBM Director	290

Chapter 9. Leveraging BladeCenter functionality	299
9.1 The Management Module in IBM BladeCenter	300
9.2 Pre-staging of chassis using virtual bays	301
9.2.1 Virtual bays	302
9.3 Rip and Replace	313
9.3.1 Rip and Replace process flow	313
9.3.2 Some considerations	314
Abbreviations and acronyms	315
Related publications	317
IBM Redbooks	317
Other publications	317
Online resources	317
How to get IBM Redbooks	319
Help from IBM	319
Index	321

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.


COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

BladeCenter®
eServer®
eServer™
IBM®

Redbooks™
Redbooks (logo) ™
RETAIN®
ServerGuide™

ServerProven®
ServeRAID™
System x™

The following terms are trademarks of other companies:

Altiris Deployment Solution, Altiris Server Management Suite, Altiris, BootWorks, Inventory Solution, PC Transplant, RapiDeploy, RapidInstall, SetupCapture, are trademarks of Altiris, Inc. in the United States, other countries, or both.

Solaris, Sun, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Active Directory, Internet Explorer, Microsoft, MS-DOS, Windows NT, Windows Server, Windows, Win32, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

i386, Intel, Pentium, Intel logo, Intel Inside logo, and Intel Centrino logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Preface

Altiris Deployment Solution is an industry leading management product which helps reduce the cost of deploying servers from bare metal and managing them all from a centralized location. Its Web-based user interface makes it easy to deploy operating systems and applications, apply custom configurations, and distribute software updates.

Deployment Solution runs in either a virtual or physical server environment and supports deploying Linux®, Windows®, and ESX Server, as well as virtual machines to an ESX Server system. Deployment Solution also integrates with the IBM® ServerGuide™ Scripting Toolkit to offer custom scripts for IBM hardware to further optimize the automation and standardization of complex server deployments on IBM hardware. Deployment Solution is a ServerProven® application and is available directly from IBM.

This IBM Redbook describes the features of Altiris Deployment Solution and explains in detail how to implement features such as managing and deploying firmware updates and hardware configuration changes, image-based and script-based deployments, and integration with the IBM management tools. This book addresses the common issues and recommends best practices to overcome many of the challenges that arise during initial deployment setup.

Update September 2006: Added 4.1.4, “Additional updates” on page 109 describing how to deploy updates such as server diagnostics using Altiris Deployment Solution and the ServerGuide Scripting Toolkit.

The team that wrote this redbook

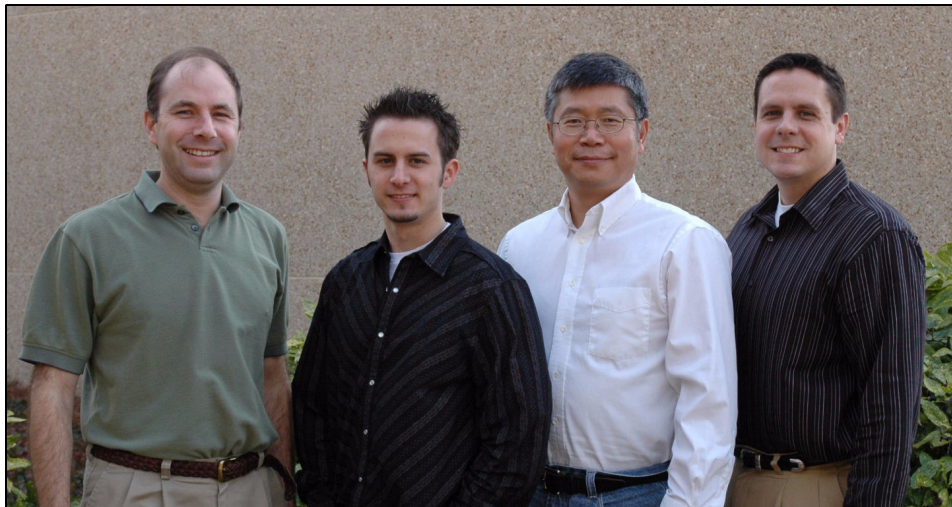
This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization, Raleigh Center.

Roland Mueller works in the Windows Solutions Lab at the IBM Center for Microsoft® Technologies in Kirkland, Washington. He is an IT Specialist and regularly works with customers from around the globe that come to Kirkland to test-drive the latest models of IBM System x™ servers. He has four years of experience in the IT industry. He holds a degree in Management Information Systems from Washington State University. His area of expertise is systems management, including IBM Director, and systems deployment, including Altiris Deployment Solution.

David Watts is a Consulting IT Specialist at the IBM ITSO Center in Raleigh. He manages residencies and produces Redbooks™ on hardware and software topics related to IBM System x servers and associated client platforms. He has authored over 40 Redbooks and Redpapers. He holds a Bachelor of Engineering degree from the University of Queensland (Australia) and has worked for IBM for over 15 years. He is an IBM Certified IT Specialist.

Terry Cheng is an Operating Systems Engineer at Wells Fargo and Company in Minneapolis, Minnesota. Terry has more than 20 years of experience in the IT field, focusing on server operating systems for the past 12 years. He holds a Bachelor of Arts degree in Electrical Engineering from Taiwan and is currently pursuing his Master of Science degree in Technology Management at the University of St. Thomas, Minnesota. Terry's areas of expertise include server operating systems, server build automation and BladeCenter® management. He also has written extensively on server build documents and technical papers.

Brian Higbee is the Strategic Alliance Manager at Altiris based in Raleigh, North Carolina. He manages the IBM relationship for Altiris where he has worked in sales and partner enablement in the systems management and life cycle management for the past seven years. He attended the University of Utah, College of Electrical Engineering and has 15 years of experience in the high tech software industry.



The team (l-r): David, Roland, Terry, and Brian

Thanks to the following people for their contributions to this project:

From the ITSO:

Tamikia Barrow
Diane O'Shea
Linda Robinson
Margaret Ticknor
Jeanne Tucker
Gabrielle Velez

From IBM:

Mary Lou Dickson
Rick Luciano
Lillian Moy
Michael Barton
Mike Trivette

From Altiris:

Rick Gines
Wendy Donovan
Hugo Parra
David Callahan

Become a published author

Join us for a two- to six-week residency program! Help write an IBM Redbook dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You'll team with IBM technical professionals, Business Partners and/or customers.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you'll develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our Redbooks to be as helpful as possible. Send us your comments about this or other Redbooks in one of the following ways:

- ▶ Use the online **Contact us** review redbook form found at:

ibm.com/redbooks

- ▶ Send your comments in an e-mail to:

redbook@us.ibm.com

- ▶ Mail your comments to:

IBM Corporation, International Technical Support Organization
Dept. HZ8 Building 662
P.O. Box 12195
Research Triangle Park, NC 27709-2195



Introduction

The benefits of a being able to quickly deploy an IBM blade server, rack mounted server, or tower server can be quickly measured by the role that the server plays in that company's environment. A downed server can cost a company millions of dollars per minute while not up and running. Alternatively, adding new servers can increase a company's productivity and capabilities by taking over new or additional functions to improve user and client experience, process payments, usage, or transactions that go straight to the bottom line.

The challenge to deploying physical servers is the complexity of the hardware and software. Configuring a server involves updating the firmware of the server, diagnostics, service processors, and adapter cards, configuring BIOS and the disk subsystem, to name just a few of the hardware challenges, that can become time consuming when faced with 5, 10, 25, or more servers.

Even if you are talking about deploying virtual servers, you still need to manage the deployment and physical characteristics defined in the virtual machine as well as installing an operating system and applications until the server is up and running. This whole process can be a complex and time consuming task.

Altiris Deployment Solution, leveraging the IBM ServerGuide Scripting Toolkit, addresses these issues on IBM BladeCenter and System x servers.

Note: IBM System x is the new name for IBM @server® xSeries®.

1.1 Altiris Deployment Solution

Altiris Deployment Solution is perhaps the most widely used deployment software for clients and servers. It has an installed base of some of the largest companies in the world who use it to deploy and managed servers and client computers alike. Whether you are remote or on-site, Altiris Deployment Solution will help you deploy the operating system, applications, and post configuration all managed by a single drag and drop from an award winning console.

Altiris Deployment Solution provides the work flow that drives and automates the manual tasks associated with deployment and configuration.

1.2 Comparing Deployment Solution with Deployment Server

Deployment *Solution* is one of the solutions that integrate into the Altiris Notification Server infrastructure, as shown in Figure 1-1 on page 3.

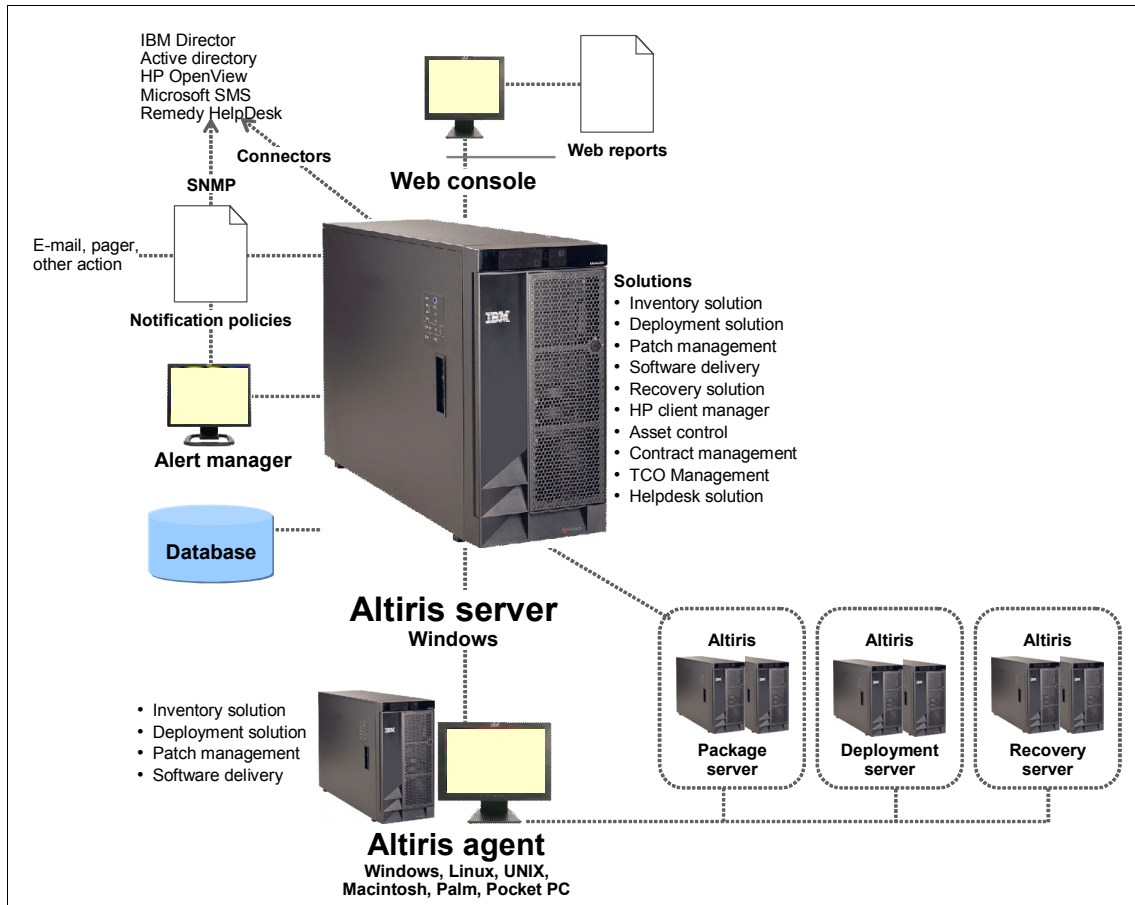


Figure 1-1 Altiris Notification Server infrastructure

Deployment Solution includes Deployment Server and the needed integration into Altiris Notification Server. Altiris Notification Server provides a Web console, Web reports, notification policies and data sharing with other Altiris Notification Server solutions creating synergist integration with the solutions so that the sum is greater than its parts.

On the other hand, Deployment *Server* is a stand alone deployment system that can run independent of the Altiris Notification Server by downloading the installation package just for windows that can be integrated at any time to Notification Server to add capabilities such as:

- ▶ Package Servers - provides local Replication points for images, applications, and updates and patches for remote sites. Package servers use Altiris Agent

trickle down technology and check point recovery and restart for successful replication over very slow links.

- ▶ Web reports - Provide several report such as Deployment Managed servers
Need more info here
- ▶ Event Notification policies - provides the capability to send and forward notification of job success or failure

1.3 Other solutions Altiris offers

Altiris Deployment Solution is part of level 1 of the Altiris Server Management Suite that contains level 3 levels. This suite starts with level 1 and progresses to level 3 and is meant for customers to adopt them in that order in order to proactively manage their environments. The levels are as follows:

1.3.1 Level 1

Level 1 of the Altiris Server Management Suite contains the following products:

- ▶ Deployment Solution for Servers - allows you to quickly and easily deploy your servers from bare metal. Pre-built deployment jobs specific for your servers provide management of hardware and system settings (including BIOS, RAID, and other component configurations) and allow you to deploy operating systems, install applications, and more- all from a central, remote console.
- ▶ Inventory Solution for servers - captures hardware information, installed software packages, and operating system settings for supported Windows, Linux, and UNIX® servers. Use this information to assess and plan for upgrades and migrations, track and manage server assets, assist with server consolidation, and verify software licensing compliance
- ▶ Application Management - collects information about product installed by Microsoft Windows Installer (MSI) and then reports the information to the Altiris Notification Server. The MSI agent helps you manage source paths, gather inventory about MSI applications, schedule regular application health check-ups and automatically repair missing or changed files or registry values.
- ▶ Software Delivery Solution - for Servers provides policy-based software distribution for applications and other software change packages throughout your organization. Software Delivery Solution also includes self-healing, conflict analysis, and other ongoing software management capabilities.
- ▶ Patch Management Solution - allows you to proactively manage patches and software updates by automating the collection, analysis, and delivery of patches across your enterprise. The solution can significantly help you

decrease the costs involved in delivering patches throughout your enterprise and integrates with Altiris Recovery Solution for stable-state rollback.

- ▶ Site Monitor Solution - watches over important network resources to ensure availability and responsiveness, such as verifying Web site content or accessibility of an Exchange server. By regularly monitoring the state of computer in the network, networked printers, and network devices, organizations can avoid costly downtime by detecting problems before users report them.
- ▶ Wise Script Toolkit - is a scripting tool that is used to perform general administrative scripting tasks (e.g. deleting temporary files, emptying the Recycle Bin, setting the value of a particular registry key, etc)

1.3.2 Level 2

Level 2 of the Altiris Server Management Suite contains the following products:

- ▶ AuditExpress for Servers is the only vulnerability audit solution that combines the traditional functions of a vulnerability scanner and the core features of an audit tool by providing security and information technology professionals with the most comprehensive functionality and the best value. AuditExpress audits your servers and delivers audit results in easy-to-understand smart reports, enabling organizations to quickly take action on identified system security vulnerabilities.
- ▶ Real Time System Manager Solution - Real-Time System Manager Solution - Real-Time System Manager Solution enables you to manage virtually any Windows computer remotely from a browser. Use Real-Time System Manager Solution to view real-time status and configuration data, and perform numerous diagnostic and management tasks from any computer with a Web browser.
- ▶ Recovery Solution for Servers - Recovery Solution for Servers protects your organization's servers with scheduled backups allowing you to recover lost data or roll back to a known good state. Protection is automatic and doesn't require user intervention. Patented technology minimizes bandwidth usage making Recovery Solution an excellent choice for protecting remote and disconnected users.

1.3.3 Level 3

Level 3 of the Altiris Server Management Suite contains the following products:

- ▶ Monitor Solution for Servers - Monitor Solution for Servers ensures server availability and reduces costs associated with server downtime through comprehensive, Web-based performance and event monitoring. Use real-time monitoring to assess current operational states, view historical data

to identify trends and isolate recurring issues, and manage problem tasks with integrated alert management.

1.4 Why IBM and Altiris

As an IBM partner, Altiris has received ServerProven certification for Deployment Solution for Servers while helping develop the integration needed for IBM servers in the IBM ServerGuide Scripting Toolkit. Combined they become Deployment Solution for IBM servers which is simply the integration of Altiris Deployment Solution for Servers and the IBM ServerGuide Scripting Toolkit.

Deployment Solution for IBM servers helps reduce the cost and complexity of deploying and managing IBM servers from a centralized location in your environment with an easy-to-use, automated solution that offers bare metal deployment of the hardware's BIOS, RAID configuration, operating system deployment, remote configuration, and software deployment of applications, updates and service packs across platforms.

As a consolidated management tool, Deployment Solution for IBM Servers integrates the IBM ServerGuide Scripting Toolkit (SSTK) with the easy-to-use, consolidated features of Altiris Deployment Solution. From a Deployment Console, you can deploy IBM BladeCenter and System x servers from bare metal by scripting or imaging Windows or Linux operating systems and VMware ESX Server, patch on both a hardware and software level, remotely deploy software such as the IBM Director Agent, rip and replace blade servers, or schedule pre-configured jobs for each phase of server management.

Altiris brings you one step closer to accomplishing these server management goals:

- ▶ Do more with less by consolidating server resources and tools.
- ▶ Prevent risk and liability by reducing manual efforts, minimizing security exposures, and integrating disaster recovery.
- ▶ Deliver value to your organization by reducing time to deploy, increasing system availability, and simplifying training.

Deployment Solution for IBM Servers offers complete and compelling features for rapidly deploying, provisioning, and repurposing IBM servers. The solution can help your IT team drive profitability, establish a competitive edge, and predict planning to reduce risk and vulnerabilities to your server environment.

Additionally, Altiris is committed to supporting the IBM Director Management platform by providing upward integration and an extension of the IBM Director Management console to Altiris Deployment Solution and the Altiris Notification

Server. This added integration will provide for added efficiency and consolidation to further reduce management costs and use the best possible hardware management and monitoring tools to get the job done.

1.5 This IBM Redbook

While Altiris Deployment Solution is an easy to use product for installation and configuration, there are still challenges that need to be overcome in personalizing this solution in any data center environment. This redbook will attempt to address the common issues and recommend best practices to overcome most of the questions and challenges that may arise during initial setup. While nothing can replace hands-on training, this redbook provides the necessary knowledge-based training when hands-on training is neither possible nor feasible given specific time or budget restrictions.

The chapters are written in the order and fashion in which someone would implement the solution into their environment, by first going through the installation and configuration of Altiris Deployment Solution, the IBM ServerGuide Scripting toolkit, loading the operating system, configuring the solution to perform hardware configuration and application installations, as well covering several advanced topics around using and leveraging the IBM BladeCenter and IBM Director.



Installation and configuration

In this chapter, we cover the installation and configuration of Altiris Deployment Solution, the ServerGuide Scripting Toolkit, and the Altiris Deployment Agent. Further, we discuss usage of the PXE pre-boot environment and the IBM Service Processor Discovery utility.

The following topics will be covered:

- ▶ 2.1, “Installing Altiris Deployment Solution 6.5” on page 10
- ▶ 2.2, “Integrating the ServerGuide Scripting Toolkit” on page 28
- ▶ 2.3, “Installation and integration of the Deployment Agent” on page 46
- ▶ 2.4, “Communicating with Deployment Solution” on page 58
- ▶ 2.5, “Configuring and using PXE pre-boot environment” on page 64
- ▶ 2.6, “Integrating with the IBM Service Processor Discovery utility” on page 69
- ▶ 2.7, “Best practices” on page 75

2.1 Installing Altiris Deployment Solution 6.5

Altiris Deployment Solution 6.5 with the IBM ServerGuide Scripting Toolkit provides a powerful tool for managing IBM System x servers through all phases of computer deployment and life cycle management.

This section covers the basic installation of Deployment Solution. Both the *Altiris Deployment Solution 6.5 Release Notes* and *Altiris Deployment Solution 6.5 Reference Guide* provide greater detail on the features, design, and installation/upgrade process. These documents can be found at the following URL:

<http://www.altiris.com/Support/Documentation.aspx>

2.1.1 Deployment Solution components

Deployment Solution is a flexible and scalable deployment and management system, made up of a number of components.

The various components that make up Deployment Solution are as follows:

- ▶ **Deployment Console:** The Deployment Console is a Win32® graphical user interface for Deployment Solution. You can install this Windows-based program on computers across the network to view and manage resources from different locations. The Deployment Console communicates with the Deployment Database and Deployment Server services. You will need administrative rights on any computer running the Deployment Console.
- ▶ **Deployment Server:** The Deployment Server controls the flow of the work and information between the managed computers and the other Deployment Server components (Deployment Console, Deployment Database, and the Deployment Share). Managed computers connect and communicate with the Deployment Server to register inventory and configuration information and to run deployment and management tasks. Computer and deployment data for each managed system is then stored in the Deployment Database. Managed computers require access to the Deployment Server at all times.
- ▶ **Deployment Database:** The Deployment Database maintains all the information about the managed computers, such as: hardware, general information, configuration, applications, services, devices, and location information.
- ▶ **Deployment Share:** A shared directory, used by Deployment Solution, where image files, RIPs, and other packages are stored. When the ServerGuide Scripting Toolkit is integrated with Deployment Solution its files are also saved in the Deployment Share. Make sure you have sufficient disk space available before installing.

- ▶ **PXE Server:** The PXE Server provides client computers on a subnet the ability to boot into an automation operating system. PXE-enabled computers will connect to the first PXE server they discover and then load the PXE boot image which contains the automation operating system along with an automation agent. The client computer's automation agent will communicate with the Deployment server and receive the job that is scheduled for that computer.
- ▶ **DHCP Server:** The DHCP server is a server set up to assign IP addresses to the client computers. This server is not an Altiris component but is required if you use PXE server.
- ▶ **Deployment Web Console:** The Deployment Web Console can remotely administer a Deployment Server installation via a Web browser. The Deployment Web Console can be installed on any server running Microsoft IIS server.
- ▶ **Deployment Agent:** To allow production level control of client computers, you can install the Deployment Agent to run on a local hard disk. The Deployment Agent communicates with the Deployment Server and registers the client in the Deployment Database.

2.1.2 Deployment Server system requirements

Deployment Solution has the following prerequisites:

- ▶ Networking
 - TCP/IP is used for network communication.
 - For Windows 2000 systems, you must set up Active Directory® with the “Permissions compatible with pre-Windows 2000” option. If you choose the option “Permissions compatible only with Windows 2000 servers,” the Deployment Server cannot manage domain accounts for you.
 - If you are using Windows 2000 only permissions, change them to the pre-2000 option from the Windows Start menu. Open. To add the Everyone group, open a command prompt and enter the following:

```
net localgroup "Pre-Windows 2000 Compatible Access" Everyone /add
```

 Restart all domain controllers for the change to take effect.
 - MTFTP (Multicast Trivial File Transfer Protocol) is needed for sending bootstrap files to managed computers in secured way.
- ▶ Operating system

Deployment Solution server components must be installed on either Microsoft Windows 2000 Server or Windows Server® 2003 as a domain member or standalone server.

► Server hardware and additional requirements:

The following table lists system requirements for each Deployment Solution component. These requirements are above and beyond the requirements of the base operating system.

Table 2-1 Deployment Server Components and system requirements

Component	Hardware	Software
Deployment Server	RAM: 256 MB Disk Space: 200 MB required	Windows 2000 Server and Advanced Server, Windows Server 2003
Deployment Console	RAM: 128 MB Disk Space: 3.5 MB	Windows 2000 Professional, Server and Advanced Server, Windows XP Professional, Windows Server 2003
PXE Server	Memory: 128 MB Disk Space: 25 MB (for boot files)	DHCP server (must be in the network, but does not have to be on the same computer as PXE server), Windows 2000 Server or Advanced Server, Windows Server 2003
Deployment Database	Memory: 128 MB Disk Space: 55 MB (for program files), plus space for data.	(Microsoft SQL Server 2000 (SP3) or MSDE 2000 (SP3))
Deployment Share	Memory: 128 MB Disk Space: 100 MB for Deployment Server program files plus space for storing files (image, boot, RIP, etc.)	Windows NT® (SP6), Windows 2000 Server or Advanced Server, Windows Server 2003, NetWare (file server only. Cannot use for any other components).
Deployment Web Console	Memory: 128 MB	Windows 2000 Professional, Server or Advanced Server, Windows XP Professional, Windows Server 2003, MS IIS 5.5, MDAC 2.71 or later.

There are three methods of installing Deployment Solution:

- Simple Deployment Solution can be installed and configured quickly with all components on a single computer. The simple install method is the most frequently used.
- Custom The various Deployment Solution components can be spread across many computers for large enterprise environments.
- Component The individual components that make up Deployment Solution can be installed individually on the same or different computers.

For further details, refer to *Altiris Deployment Solution 6.5 Reference Guide*.

Note: Altiris supports Microsoft SQL Server 2000 SP3 or higher. You should install SQL Server 2000 before Altiris installation. At the time of writing SQL Server 2005 was not supported.

2.1.3 Simple installation

Simple Install is a procedure that places all Deployment Server components, such as the Deployment Server, the Deployment Console, the Deployment Share, and the Deployment Database, on the same computer.

Note: Simple install works only with a default Microsoft SQL Server 2000 or MSDE 2000 install. Using the Simple Install option, you have to install Microsoft SQL 2000 or MSDE 2000 on the local computer first if a database is not already installed. A customized Microsoft SQL Server installation will not work with the simple install. Simple Install Helper will check and install required third-party software on local computer.

To perform a simple installation of Altiris Deployment Solution 6.5 perform the following steps:

1. Log on to the computer you have designated as your new Deployment Server using an account with local administrator privileges.
2. Run the Altiris Deployment Solution executable you obtained from Altiris. This opens the Altiris Packager Self-Extracting Executable Options window. Click **Extract & Execute App**, located in the upper-right portion of the window. This launches the installation of Deployment Solution. If you want to simply extract the installation files, you can use the **Extract Only** button. Also, you can control the folder where the installation files will be saved by altering the file path in the text box for **Extract to a specific folder**.

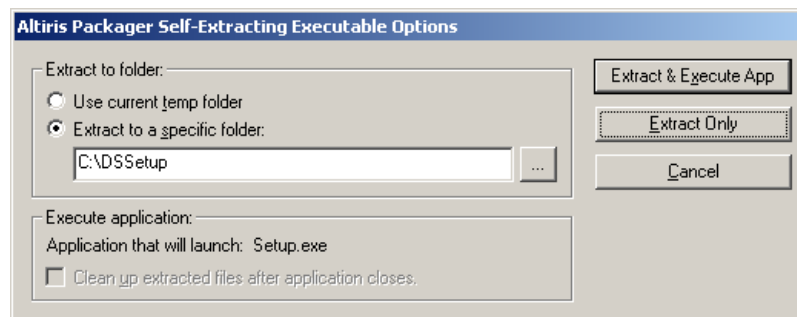


Figure 2-1 The Altiris Packager Self-Extracting Executable Options window

3. When the Deployment Server Install Configuration window loads (as shown in Figure 2-3 on page 15), select **Simple Install Helper** and then click **Install** to verify that all third-party software has been installed.

Note: If you ever need to access the Deployment Server Install Configuration window again, you can do so by running the axInstall.exe file located in the directory where you extracted the installation files in Figure 2-1.

If all third-party software has been installed, you should see a window like that shown in Figure 2-2.

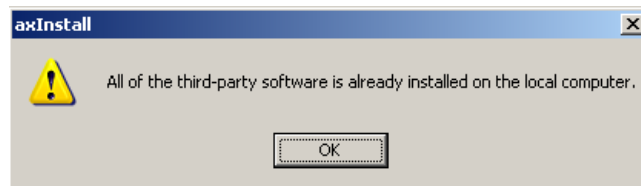


Figure 2-2 A window showing that all third-party software has been installed

4. To continue with the simple install, select **Simple Install**. If you would also like to install the Altiris PXE Server check the check box labeled **Include PXE Server**. Click **Install** to begin installation.

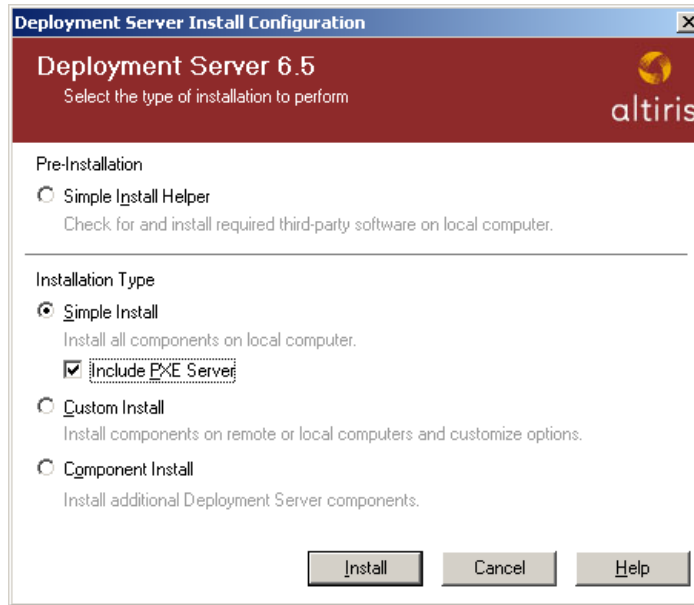


Figure 2-3 Deployment Server Install Configuration window with Simple Install with PXE Server

5. Click **Yes** to agree to the Software License Agreement and continue.
6. When the Deployment Share Information window loads, enter a path to install the Deployment Server in **File server path**. To create a Deployment Share, select **Create Deployment Share**. In the next section of the window you have the option to use a free seven day license to operate the Deployment Server or to add a license you have obtained from Altiris.

If you have obtained a license from Altiris, click **Browse** and navigate to the license file (.lic). Finally, add a local user name with local administrative privileges in the **Service user name** text box. For **Service Password**, enter a password for the user account you just entered. Click **Next** to continue.

Note: It is a best practice to use a local administrator account with the Password never expires option set in Windows.

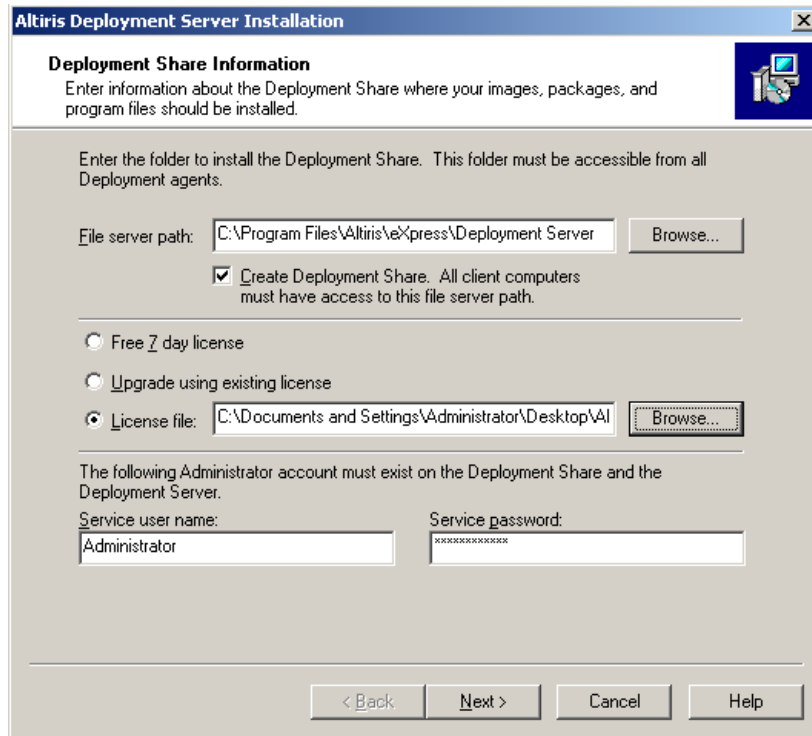


Figure 2-4 Deployment Share Information window

7. The Pre-Boot Operating System window loads. In this window you have the option to load the various pre-boot operating systems that can be used by the PXE Server to manage computers.

We recommend you load MS-DOS® files to create an MS-DOS PXE boot disk. To do so, select **MS-DOS**, then click the enabled **Browse** button. Navigate to the location of your MS-DOS files and click **OK**. The table below lists the required MS-DOS files to create a MS-DOS PXE boot disk. Click **Next** to continue.

Table 2-2 Required MS-DOS files

Required Files	Supporting Files
IO.SYS MSDOS.SYS HIMEM.SYS EMM386.EXE SMARTDRV.EXE COMMAND.COM SYS.COM	FORMAT.COM EDIT.COM FDISK.EXE MEM.EXE ATTRIB.EXE XCOPY.MOD

Note: Pre-boot operating system files can be added at a later time through the Boot Disk Creator if you choose not to add them during the installation.

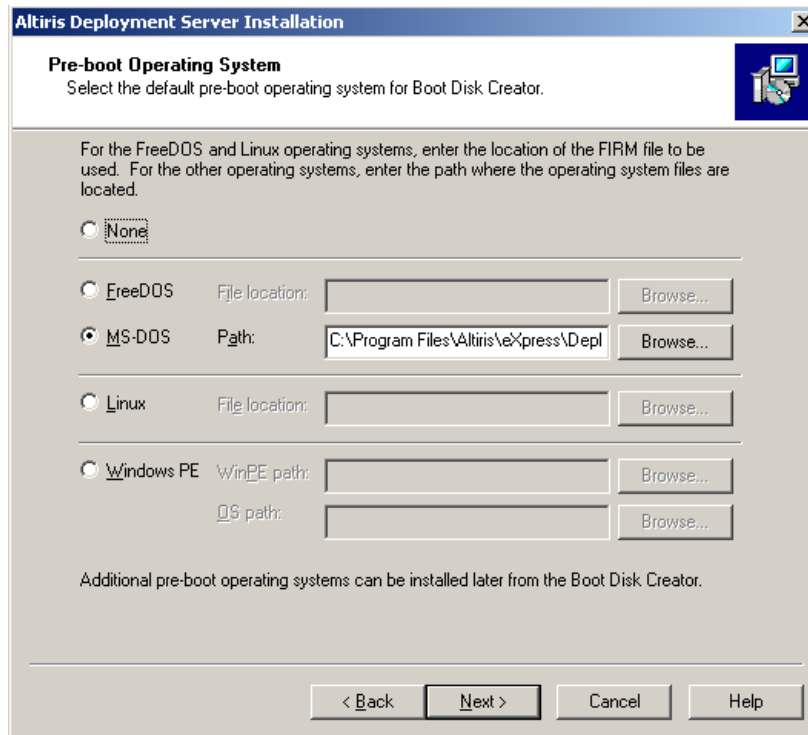


Figure 2-5 The Pre-Boot Operating System window

8. When the Installation Information window loads, click **Install** to begin the installation.
9. After the installation completes, the Installation Summary window will load, Figure 2-6 on page 18, giving you the option to integrate Microsoft Sysprep, to remotely install the Deployment Agent, and to download Adobe Acrobat for reading Altiris documentation.

Note: These features can be installed later if you wish.

We recommend you integrate Microsoft Sysprep to aid in the imaging process. Integration with Microsoft Sysprep is covered in-depth in 6.4, “Integrating Sysprep with Deployment Solution” on page 193. For now, we will

leave the check box for **Enable Microsoft Sysprep support** unchecked and continue with the installation.

If you want to remotely deploy the Deployment Agent, check **Remotely install Deployment Agent**.

If you want to download Adobe Acrobat Reader, and your Deployment Server has a connection to the Internet, check **Download Adobe Acrobat Reader**.

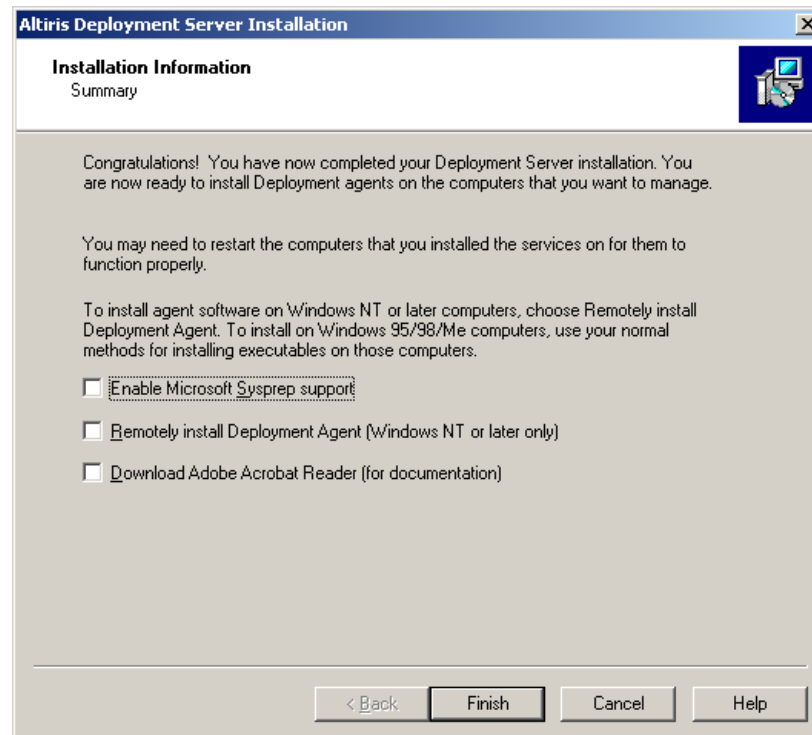


Figure 2-6 The Installation Information Summary window

10. Click **Finish** to complete the simple installation.

2.1.4 Custom installation

The Custom Install option allows you to distribute the various Deployment Solution components among many computers for large enterprise environments.

To perform a custom installation follow the steps listed below:

1. Complete steps 1 through 3 of the simple install in 2.1.3, “Simple installation” on page 13.

2. On the Deployment Server Install Configuration window shown in Figure 2-3 on page 15, select **Custom Install**. Click **Install** to begin the installation.
3. Click **Yes** if you agree to the Software License Agreement.
4. Fill out the Deployment Share Information window as described on page 15. Click **Next** to continue.
5. When the second Deployment Server Information window loads you have the option to install the Deployment Server on the local computer or on a remote computer.

The screenshot shows a window titled "Altiris Deployment Server Installation" with a sub-header "Deployment Server Information". Below the sub-header is the instruction "Enter information about the Deployment Server." and a small icon of a computer. The main area contains the question "Where would you like to install the Deployment Server?" with two radio buttons: "On this computer" (selected) and "On a remote computer". Below the "On a remote computer" option is a text box for "Remote computer name:" and a "Browse..." button. Further down are text boxes for "IP address:" (containing "192 . 168 . 55 . 1"), "Port:" (containing "8080"), and "Deployment Server install path:" (containing "C:\Program Files\Altiris\express\Deployment Server"). Below these is a note: "The following Administrator account must exist on the Deployment Share and the Deployment Server. If using Active Directory, enter 'domain\user name'." This is followed by two text boxes: "Service user name:" (containing "Administrator") and "Service password:". At the bottom are four buttons: "< Back", "Next >", "Cancel", and "Help".

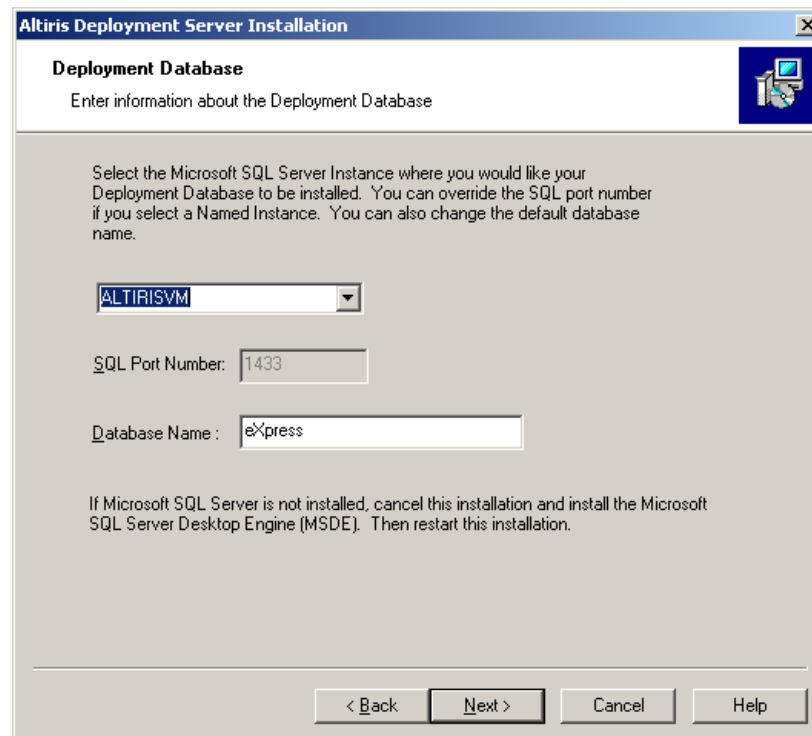
Figure 2-7 Deployment Server Information window of the custom installation process

Since this is a custom install we will assume you want to install the Deployment Server on a remote computer. Select **On a remote computer** and in the **Remote computer name** field, enter the NetBIOS name (or IP address) of the computer on which you want to install the Deployment Server or click **Browse** to locate the computer. In the **IP address** field, enter a static IP address for the Deployment Server computer (use static addressing to ensure that the IP address remains constant). Type the port information in the **Port** text box. Finally, add a local user name with local administrative

privileges in the **Service user name** text box. For **Service Password**, enter a password for the user account you just entered. Click **Next** to continue.

6. The install will attempt to locate an existing SQL Server in your environment. When the Deployment Database window loads the information should be pre-populated. If not, enter the name of the SQL Server instance you want to use in the first text box. Enter the name of the database you want to use in the **Database Name** text box (eXpress is the default value).

Note: The information in Figure 2-8 is for display only, not the default values. They were pre-populated by the install after examining our test environment. Please define your own instance, port number and database name to match your own environment.



The screenshot shows a window titled "Altiris Deployment Server Installation" with a sub-header "Deployment Database". Below the sub-header is the instruction "Enter information about the Deployment Database". The main area contains a paragraph: "Select the Microsoft SQL Server Instance where you would like your Deployment Database to be installed. You can override the SQL port number if you select a Named Instance. You can also change the default database name." Below this are three input fields: a dropdown menu with "ALTIRISVM" selected, a text box for "SQL Port Number" containing "1433", and a text box for "Database Name" containing "eXpress". At the bottom, there is a paragraph: "If Microsoft SQL Server is not installed, cancel this installation and install the Microsoft SQL Server Desktop Engine (MSDE). Then restart this installation." and four buttons: "< Back", "Next >", "Cancel", and "Help".

Figure 2-8 Deployment Database window of the custom installation process

7. When the Gathering Information window loads, decide on the type of authentication to be used to access the SQL Server database. You have the option of using Windows NT or SQL Server authentication. Select the radio button of your choosing and then click **Next**.

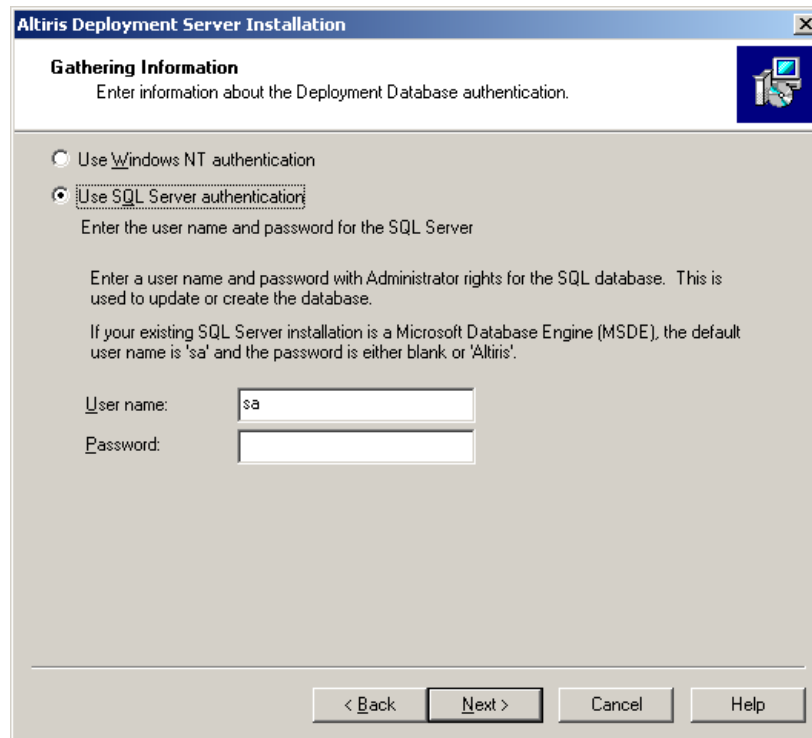


Figure 2-9 Gathering Information window of the custom installation process

8. When the Pre-boot Operating Systems window loads, fill out the fields as done on step 7 on page 16.
9. When the PXE Server Information window loads, you are given the option to skip the PXE Server install, to install the PXE Server on the local computer, or to install the PXE Server on a remote computer. Select the radio button of your choice.

In this example we are installing the PXE Server on a remote computer and have selected the appropriate radio button (see Figure 2-10 on page 22). If you are installing the PXE Server on a remote computer enter the NetBIOS name or IP address of the computer you have designated as your PXE Server for **Remote computer name**. In this example our PXE Server's NetBIOS name is ALTIRISPXE. In the **PXE Server IP address** text box, enter a static IP address for the PXE Server. The next field, **Deployment Server IP address**, is auto-populated with the IP address you entered in the Deployment Server Information window (shown in Figure 2-7 on page 19). Verify that the install path is correct in the **PXE Server install path** text box. Finally, select the pre-boot operating system you want to use as your default

PXE menu boot option by selecting the radio button of your choice (DOS, Linux, or Windows PE). Click **Next** to continue.

Note: Since we loaded only the MS-DOS pre-boot operating system files during the install, it is the only option enabled in this window. If we had loaded Linux or Windows PE those options would also have been enabled.

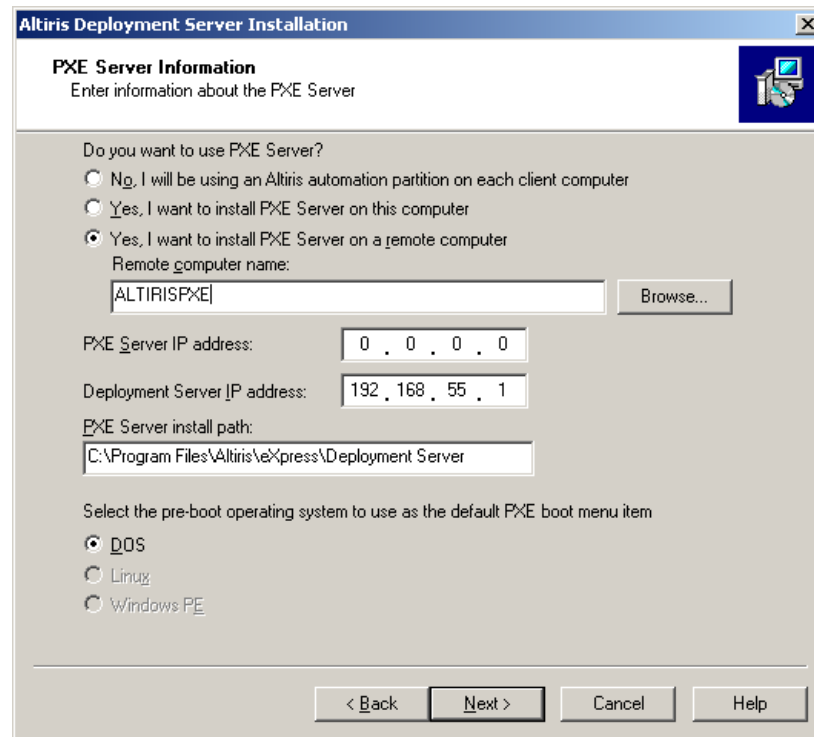


Figure 2-10 PXE Server Information window of the custom installation process

10. The Deployment Agent Connection to Deployment Server window allows you to specify the method of communication between the Deployment Agent on the client computer, and the Deployment Server.

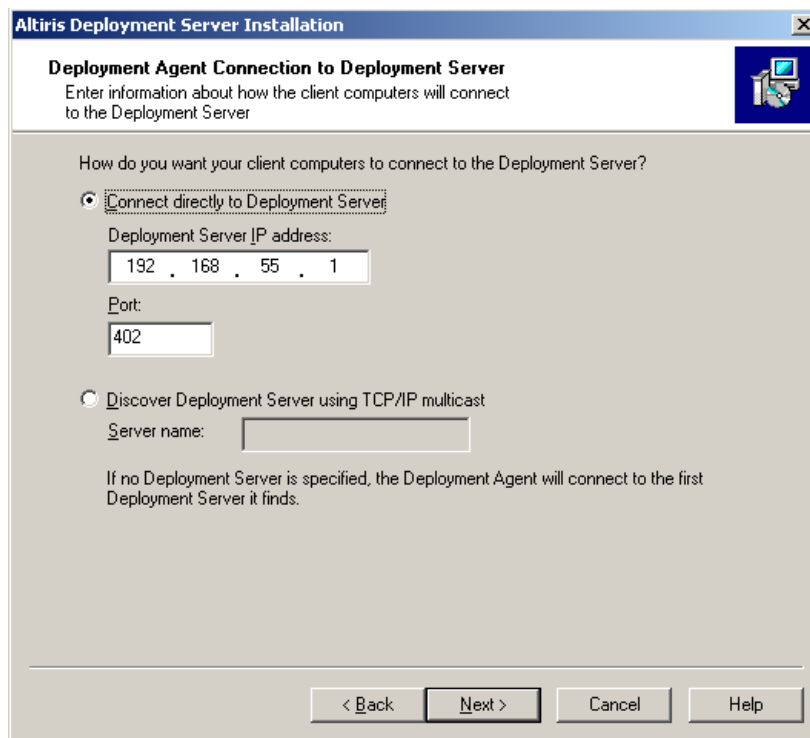


Figure 2-11 Deployment Agent Connection window of the custom installation process

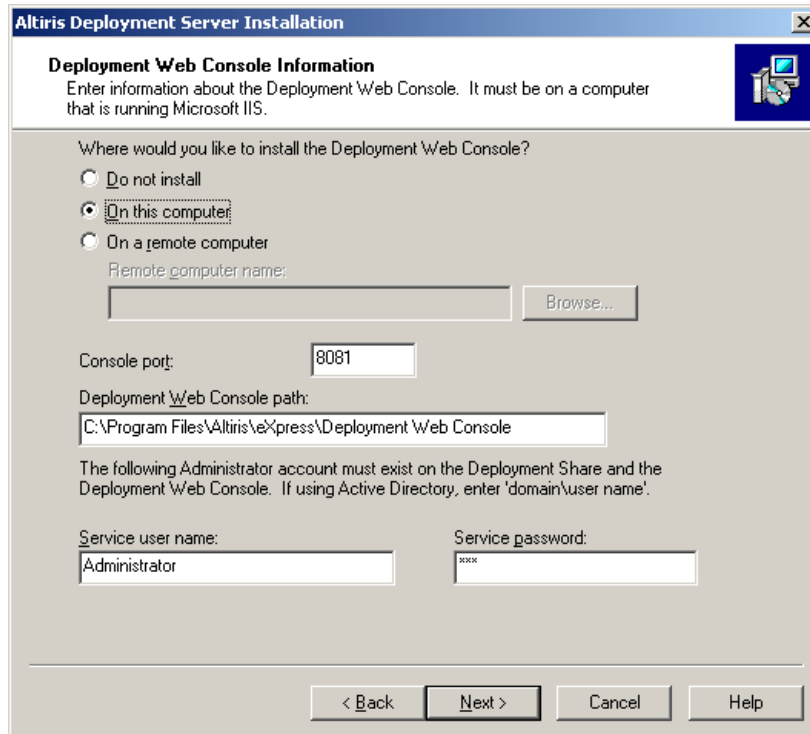
The two options are by using the IP address of the Deployment Server or by using multicast and the NetBIOS name of the Deployment Server. Select the radio button for the method that applies to your environment.

- If you selected **Connect directly to Deployment Server**, enter the IP address of the Deployment Server in the text box provided.
- If you would rather search for the Deployment Server using multicast and the NetBIOS name, select **Discover Deployment Server using TCP/IP multicast**, and enter the NetBIOS name of the Deployment Server.

Click **Next** to continue.

11. The Deployment Console window is very simple. It asks whether you want to install the Deployment Console on the local or a remote computer. Select one of the two radio buttons. If you selected **On a remote computer**, enter the NetBIOS name or IP address of the remote computer. Click **Next** to continue.

12. When the Deployment Web Console window loads you have three options: not installing the Deployment Web Console, installing it on the local computer, or installing it on a remote computer. In this example we will install the Deployment Web Console on the local computer. Verify the install path in the **Deployment Web Console path** text box. Finally, enter a user account with local administrative privileges in the **Service user name** text box. Finish by entering a password for the user account you provided in the **Service password** text box. Click **Next** to continue.



The screenshot shows a Windows-style dialog box titled "Altiris Deployment Server Installation". The main heading is "Deployment Web Console Information". Below the heading, it says "Enter information about the Deployment Web Console. It must be on a computer that is running Microsoft IIS." There are three radio button options: "Do not install", "On this computer:" (which is selected), and "On a remote computer:". Below the "On a remote computer:" option is a text box for "Remote computer name:" and a "Browse..." button. The "Console port:" is set to "8081". The "Deployment Web Console path:" is "C:\Program Files\Altiris\Express\Deployment Web Console". Below this, a note states: "The following Administrator account must exist on the Deployment Share and the Deployment Web Console. If using Active Directory, enter 'domain\user name'." There are two text boxes: "Service user name:" containing "Administrator" and "Service password:" containing "XXXX". At the bottom, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

Figure 2-12 Deployment Web Console Information window of the custom installation process

Note: The Deployment Web Console must be installed on a computer that is running Microsoft IIS.

13. When the Installation Information window loads, click **Install** to begin the installation. The installation process might take several minutes to complete.

14. After the installation process completes, the Installation Information Summary window loads as shown in Figure 2-6 on page 18. Click **Finish** to complete the installation.

2.1.5 Component installation

The option to install individual components can be used to install additional Deployment Consoles, Deployment Web Consoles, PXE Servers, Deployment Agents, or to integrate with Microsoft Sysprep.

Since the component installation is a subset of the custom installation method it will not be covered heavily in this document.

To begin a component installation follow the steps below:

1. Complete steps 1 through 3 of the simple installation in 2.1.3, “Simple installation” on page 13.
2. On the Deployment Server Install Configuration window shown in Figure 2-3 on page 15, select **Component Install**. Click **Install** to begin the installation.
3. On the Deployment Share Information window, enter the path to the Deployment Share. Click **Next** to continue.
4. Select the components you want to install as shown in Figure 2-13 on page 26 and click **Next** to continue.

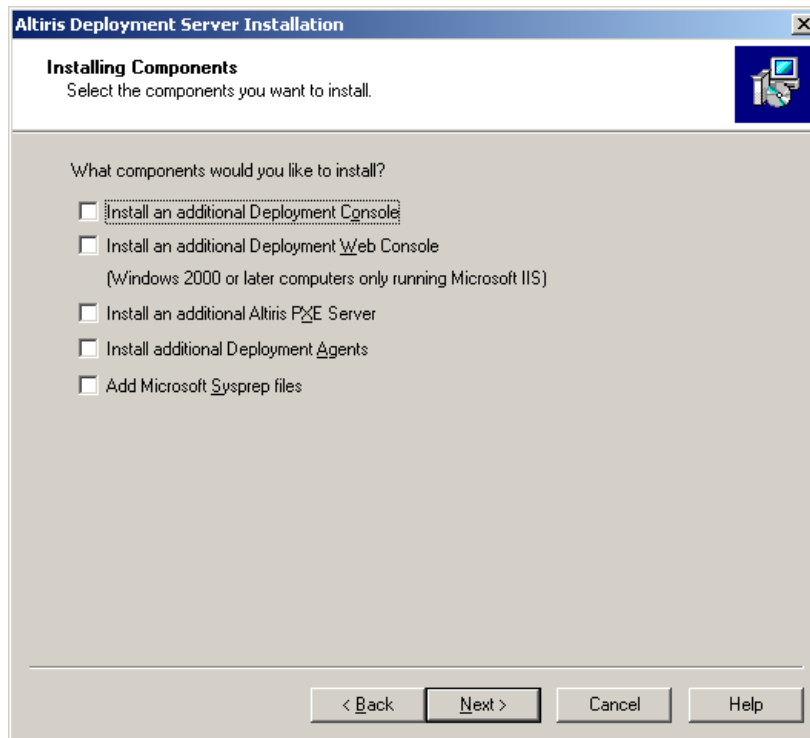


Figure 2-13 Installing Components window of the component installation process

Refer to the installation steps in 2.1.4, “Custom installation” on page 18 for an overview of the various installation windows.

Note: Refer to *Altiris Deployment Solution 6.5 Reference Guide* for further customized configurations of components to best fit your environment.

2.1.6 Installing Altiris hotfixes

Altiris always recommends that you download the latest service packs and hotfixes from the following URL if applicable.

<http://www.altiris.com/support/updates/>

Note: At the time of writing, Deployment Solution 6.5 Hotfix 2 is current and needs to be installed separately after Deployment Solution for Servers 6.5 has been installed.

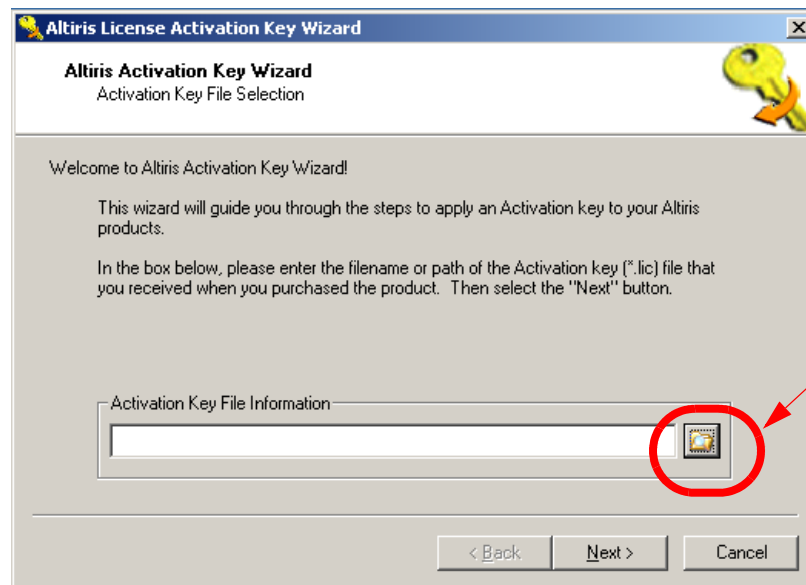
2.1.7 Applying license activation keys

Before a new client computer can be managed, the Deployment Server must have a license activation key that is not currently being consumed by a different client computer.

Activation keys can be obtained through Altiris or through IBM. Activation Keys come in the form of a license file (.lic). Talk with your account representative to obtain these license files.

Follow these steps to apply any Activation Keys you have received:

1. Close the Deployment Console
2. Click **Start** → **Programs** → **Altiris** → **Deployment Solution** → **Product License Utility**
3. When prompted with the Altiris Activation key Wizard, browse to your Activation Key (*.lic). When you have located your license file, click **Next** to continue.



Click here to browse to your Activation Key.

Figure 2-14 Altiris License Activation Key Wizard

4. A summary window will load showing the details of the license file. If everything is correct, click **Next** to continue. If this is not the correct license file you can click **Back** to return to the previous window.
5. The next window lists the Altiris products that will be affected by the new Activation Key. If you are using an Activation Key that expires, you have the

option to replace all existing license Activation Keys with the new key. If you want to replace all existing keys, check **Replace all license Activation Keys with this new Activation Key**. If you choose not to replace the existing Activation Keys with the new key, leave the check box unchecked and click **Finish**. The new Activation Key will be still be added.

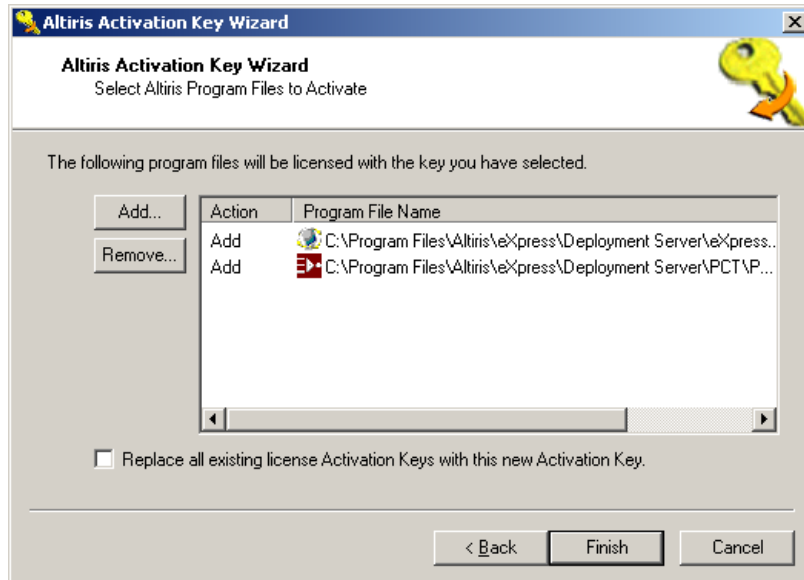


Figure 2-15 Altiris Activation Key Wizard listing Altiris products that will be licensed

6. On the final summary window, click **Done** to complete the process.

2.2 Integrating the ServerGuide Scripting Toolkit

The ServerGuide Scripting Toolkit is a collection of system configuration tools and installation scripts that you can use to deploy operating systems to BladeCenter or System x computers in a repeatable and predictable manner. The ServerGuide Scripting Toolkit and Altiris Deployment Solution together help automate computer provisioning and maintenance. The IBM ServerGuide Scripting Toolkit provides Deployment Solution with sample scripts that utilize powerful ServerGuide tools creating a consolidated deployment and provisioning management tool.

From the Deployment Console, you can provision IBM BladeCenter and System x Servers from bare metal by scripting or imaging Windows or Linux operating systems, updating both at the hardware and software level, remotely deploying

applications such as the IBM Director Agent, or scheduling pre-configured jobs for each phase of the computer management life cycle.

The *IBM ServerGuide Scripting Toolkit User Reference* publication provides detailed information about installing, configuring and using the IBM ServerGuide Scripting Toolkit. For more information and to download documentation visit:

http://www.ibm.com/servers/eserver/xseries/systems_management/sgstk.html

Tip: To access the User Reference manual, click the link in the top right corner of the Web page listed above, then scroll to the very bottom of the subsequent page.

With addition of the ServerGuide Scripting Toolkit, you can perform additional tasks through the Deployment Console:

- ▶ Update System BIOS
- ▶ Update RAID BIOS/firmware
- ▶ Configure supported RAID controllers
- ▶ Perform server secure disposal
- ▶ Configure Fibre Channel Host Adaptors (HBA)
- ▶ Perform scripted operating system installations with ServerGuide device driver integration
- ▶ Perform imaged operating system installations
- ▶ Update device drivers
- ▶ Install applications such as the IBM Director agent

Note: Some jobs require customizing. New jobs can be created using the sample jobs as templates.

2.2.1 Installation of the ServerGuide Scripting Toolkit

Before installing the ServerGuide Scripting Toolkit, you need to obtain the executable from the IBM Web site. You can download the latest IBM ServerGuide Scripting Toolkit installer from the following URL:

http://www.ibm.com/servers/eserver/xseries/systems_management/sgstk.html

To install the SGTk follow the steps outlined below:

1. Double-click the executable to initiate the install process. After the usual welcome and license agreement screens, you will see Figure 2-16 on page 30, the Usage Selection window. To integrate with Deployment Solution,

select **Integrate with Altiris Deployment Solution, Windows version**. Click **Next** to continue.

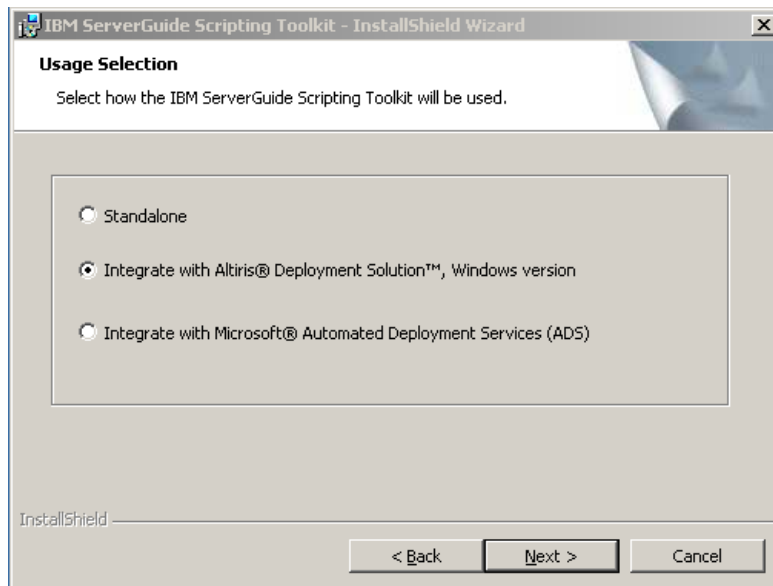


Figure 2-16 SGTK Usage selection window

2. In the Destination Folder window, verify the SGTK installs into the path of the Deployment Share. Click **Next**.
3. Click **Install** to begin the installation.

Note: If you are installing to a drive other than C:, a window with Error 1722 may appear as shown in Figure 2-17. This is a known issue with Version 1.3 as described in the following RETAIN® tip:

<http://www.pc.ibm.com/support?page=MIGR-62782>

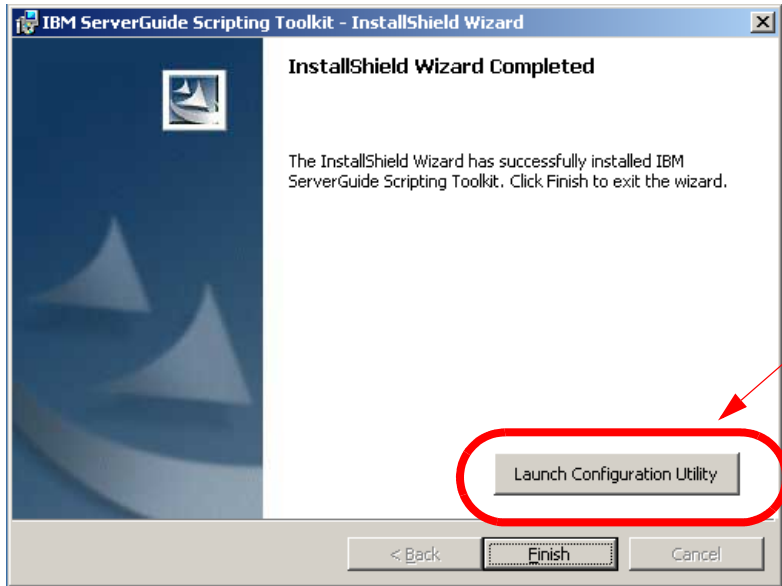
See the work around information in the above URL to determine the steps you need to take or just follow the steps in “Manually importing ServerGuide Scripting Toolkit sample jobs” on page 34. Click **OK** to continue. This issue is fixed with Version 1.3.02.



Figure 2-17 Error message when installing the SGTK to a drive other than C:

4. On the final window there is an option that often goes overlooked during the SGTK install; the option to launch the Configuration Utility. Click **Launch Configuration Utility** to open a wizard to help import various media required by the SGTK (operating system installation files, device drivers, application files, etc.). The Configuration Utility is also accessible from the Deployment Console when the SGTK has been installed. If you would rather configure the SGTK later, click **Finish** to complete the installation. Section 2.2.2, “Configuring the ServerGuide Scripting Toolkit source tree” on page 35 covers the Configuration Utility.

Note: To access the SGTK Configuration Utility from the Deployment Console click **Tools** → **IBM Tools** → **IBM Toolkit Configuration utility** from the main menu of the Deployment Console.



Click this to launch the Configuration Utility during the SGTK install process.

Figure 2-18 Install Shield Wizard Completed window

Changes made to the Deployment Console

Integration of the ServerGuide Scripting Toolkit makes a few changes to the Deployment Console: a new option is added to the Tools menu and new sample jobs are added to the Jobs pane.

If the installation was successful, you will see a new option under the Tools menu: **IBM Tools**. The ServerGuide Scripting Toolkit Configuration Utility can be initiated by clicking **Tools** → **IBM Tools** → **IBM Toolkit Configuration Utility** as shown in Figure 2-19 on page 33.

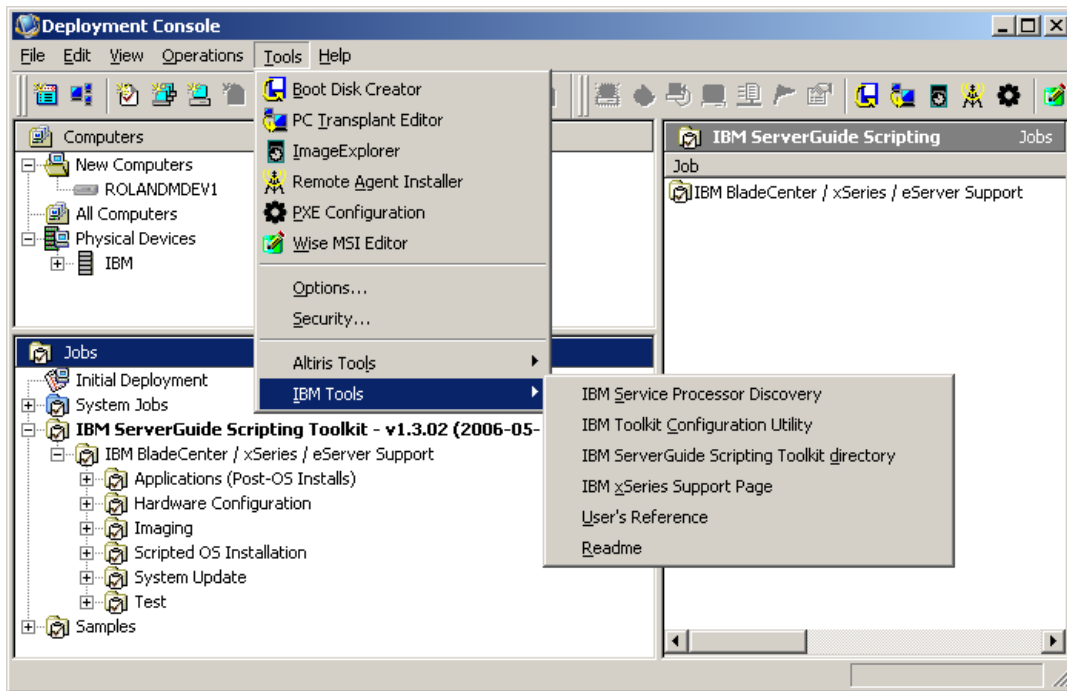


Figure 2-19 New menu options in the Tools menu

When the SGTK is installed, a new folder containing sample jobs is added to the Deployment Console's Jobs pane. The folder is labeled **IBM ServerGuide Scripting Toolkit - VersionNumber (DateReleased)**, where *VersionNumber* is the version number of the SGTK and the *DateReleased* is the date the SGTK was released to the Web.

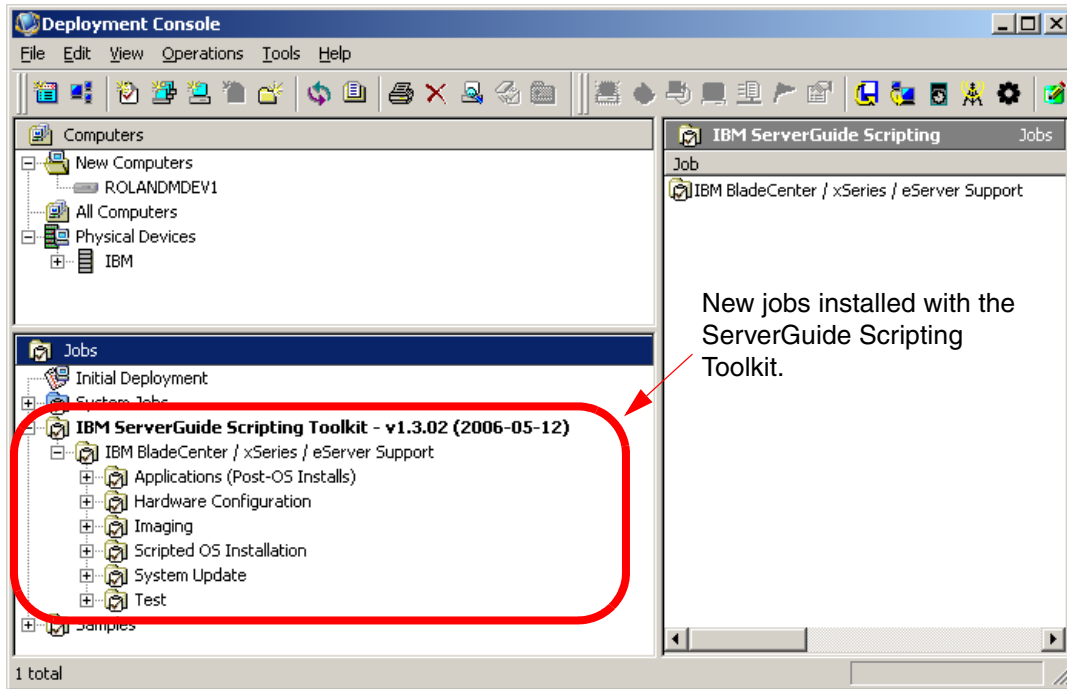


Figure 2-20 Deployment Console showing new jobs added by integration with the SGTK

Manually importing ServerGuide Scripting Toolkit sample jobs

Important: Version 1.3 of the ServerGuide Scripting Toolkit sometimes requires you to manually import the sample jobs. If you received a 1722 error, shown in Figure 2-17 on page 31, during the install you must import the jobs manually. This section covers the manual importing of SGTK jobs. If you did not see the 1722 error you can skip this section.

To manually import the sample jobs that are installed with the ServerGuide Scripting Toolkit follow the steps below:

1. Highlight the Jobs pane in the lower left portion of the Deployment Console.
2. On the main menu, click **File** → **Import/Export** → **Import Jobs**.
3. Navigate to the altiris folder inside the SGTK source tree (the sgdeploy folder), which is located in the Deployment Share:

```
<Altiris server installation drive>\Altiris\Express\Deployment
Server\sgdeploy\sgtk\altiris
```


4. Select the **ServerGuideToolkit-AltirisDSForWindows.bin** file and click **Open**.
5. On the Import Job window, check **Import Job Folder** to import the jobs to the folder name specified in the text box to the right. The next two check boxes give you the options to overwrite existing jobs, or to delete all existing jobs in the folder you specify. Click **OK** to import the jobs.

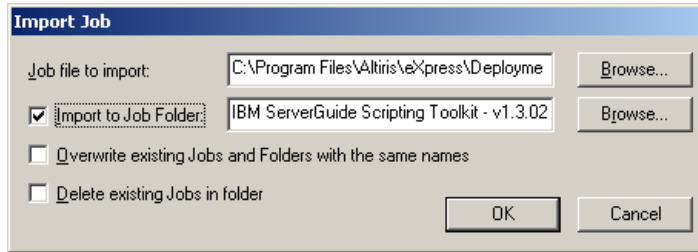


Figure 2-21 Import Job window

2.2.2 Configuring the ServerGuide Scripting Toolkit source tree

The source tree is a set of directories that contains the files used by the ServerGuide Scripting Toolkit to configure hardware and deploy operating systems. The folder named sgdeploy is the root folder of the source tree and by default is located in the Deployment Share. Before using the SGTK, you must copy operating system installation files, device driver files, and application files to the source tree.

The SGTK provides the Configuration Utility to aid in the populating of the source tree. To initiate the Configuration Utility open the Deployment Console and click **Tools** → **IBM Tools** → **IBM Toolkit Configuration Utility** from the main menu. The Configuration Utility is shown below.

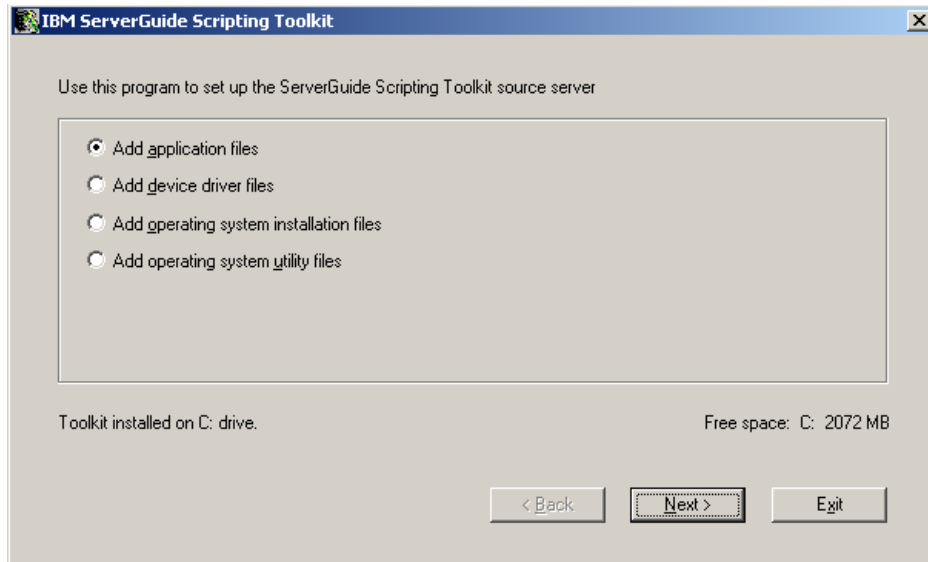


Figure 2-22 The start window of the Configuration Utility

The start window gives you the following options:

- ▶ Add application files
- ▶ Add device driver files
- ▶ Add operating system installation files
- ▶ Add operating system utility files

The following sections will cover each of these options in-depth. To initiate each option select the radio button next to your choice and click **Next**.

Add application files

The Add applications files option gives you the ability to add application install files to the SGTK source tree. Currently, the only option is IBM Director Agent 5.10.

Follow the steps outlined below to add the Director Agent install files to the source tree:

1. Click **Next** to add the IBM Director Agent 5.1 installation files to the source tree.

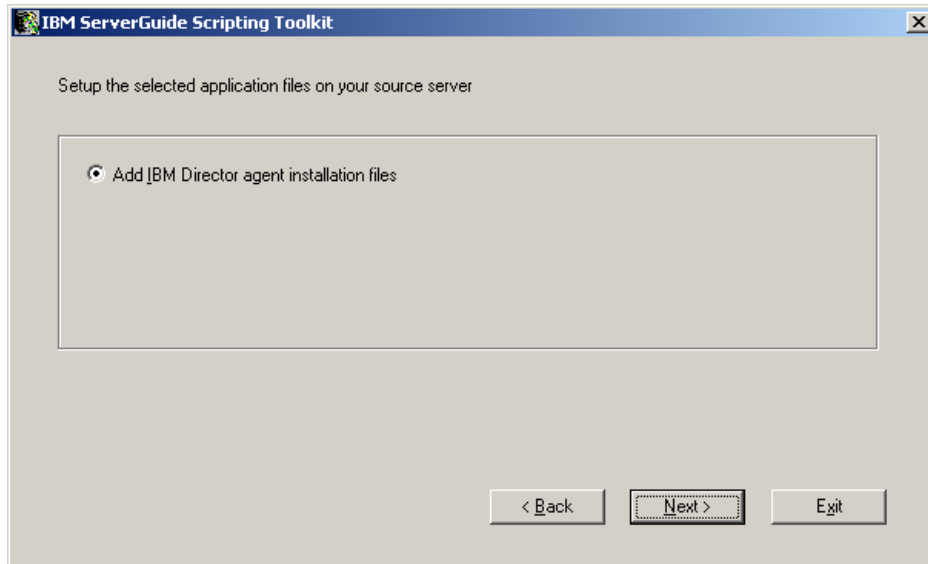


Figure 2-23 Adding application installation files

2. In the next window specify the location of the Director Agent files, either from the installation media or from an executable obtained from the IBM Web site, by selecting the corresponding radio button. Click **Next** to continue.

Note: If you are using an executable obtained from the IBM Web site, the file must be extracted first.

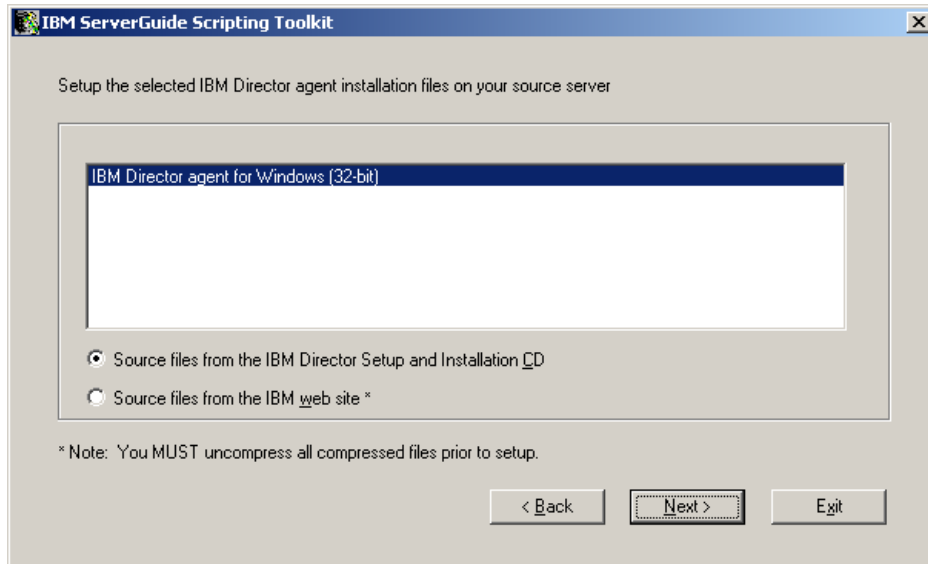


Figure 2-24 Specify the location of the IBM Director source files

3. If you selected to use the installation media as the source of the IBM Directory Agent the window shown in Figure 2-25 on page 39 will load. In the **Source Path** text box, point to the location of the installation media. The **Target Folder** text box lists the folder within the SGTK source tree to save the install files. Click **Next** to continue.

Important: We do not recommend changing the variable in the Target Folder text box. This will break some sample jobs that are installed with the ServerGuide Scripting Toolkit.

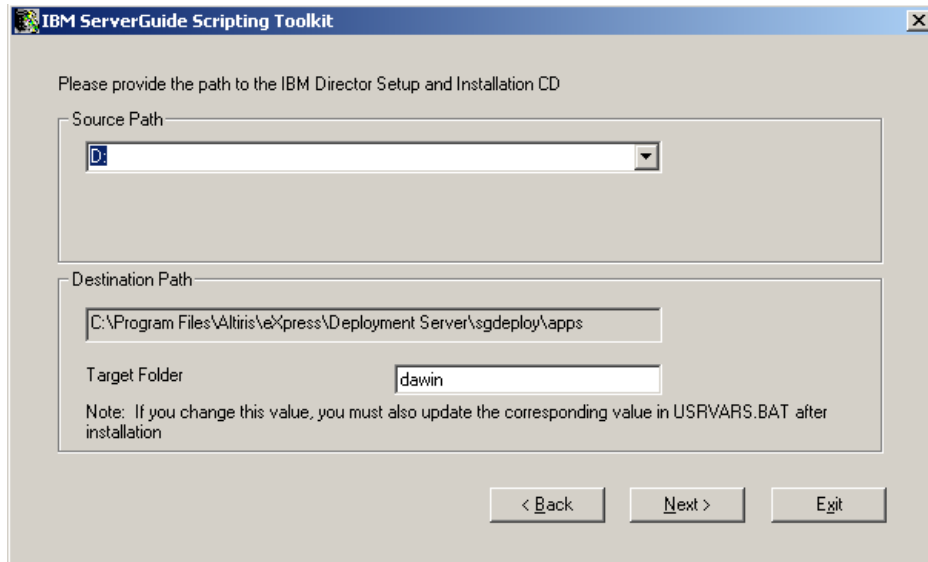


Figure 2-25 Installing the IBM Director Agent from the installation media

4. When the small TKConfig window loads, click **OK** to complete the installation of the IBM Director Agent install files.
5. If you selected **Source files from the IBM Web site** as your source for the IBM Director Agent installation files, the window shown in Figure 6 on page 40 will be displayed. Extract the downloaded file to a floppy disk (or other location) and then verify the **Source Path** text box, correctly points to the installation media. Click **Next** to continue.

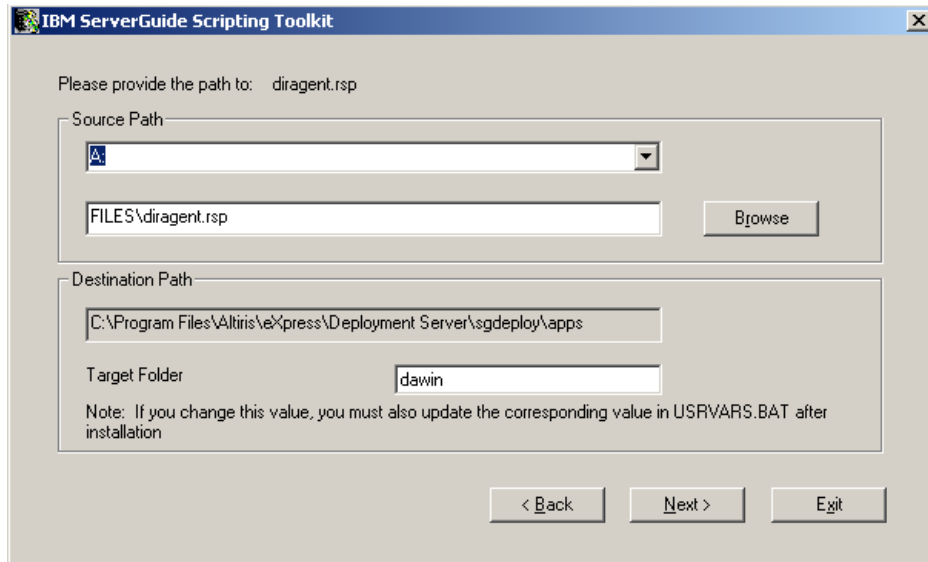


Figure 2-26 Installing the IBM Director Agent from a downloaded file

6. When the small TKConfig window loads, click **OK** to complete the installation of the IBM Director Agent install files.

Add device driver files

Add device driver files as follows:

1. There are two options for adding device driver files: adding drivers for Windows 2000 or for Windows 2003. Select **Device driver files for Microsoft Windows 2000** or **Device driver files for Microsoft Windows 2003**. Click **Next**.

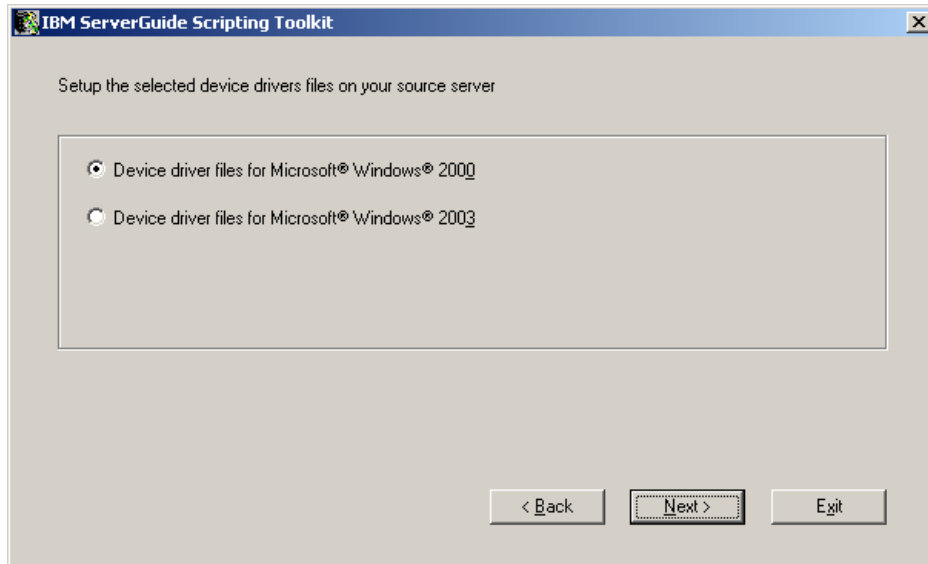


Figure 2-27 Installing device driver files for Windows 2000 or Windows 2003

2. Make sure ServerGuide CD media is in CD-ROM, and verify that the path in the **Source Path** text box correctly points to the CD-ROM drive. The variable in the **Target Folder** text box points to the folder in the SGK source tree where the drivers will be saved. The default target path is highly recommended. Click **Next** to begin the install.

Tip: Take advantage of the Remote Supervisor Adapter II in many System x computers or the Management Module in the IBM BladeCenter chassis. If you don't normally physically sit in front of your Deployment Solution computer, use the remote control function of these service processors to mount the CD-ROM drive of your desktop PC to the computer running Deployment Solution and the ServerGuide Scripting Toolkit.

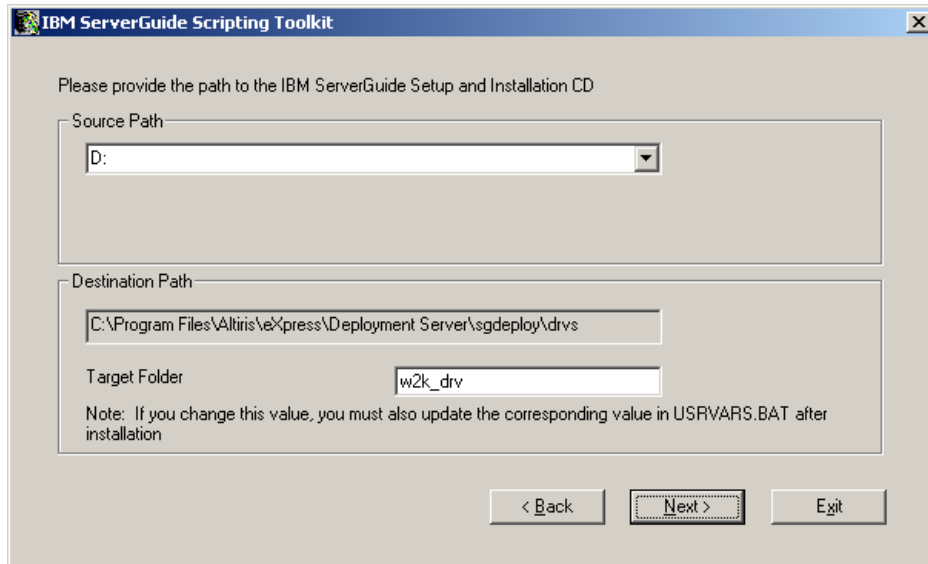


Figure 2-28 Select the install source path and target folder

3. When the TKConfig window loads, click **OK** to complete the install of the device driver files.

Add operating system installation files

Add operating system installation files as follows:

1. Select your choice of operating system, Windows, Red Hat Linux, or SUSE Linux, by selecting the distribution's corresponding radio button. In this example we will cover Windows 2003 Server Enterprise Edition. Click **Next**.

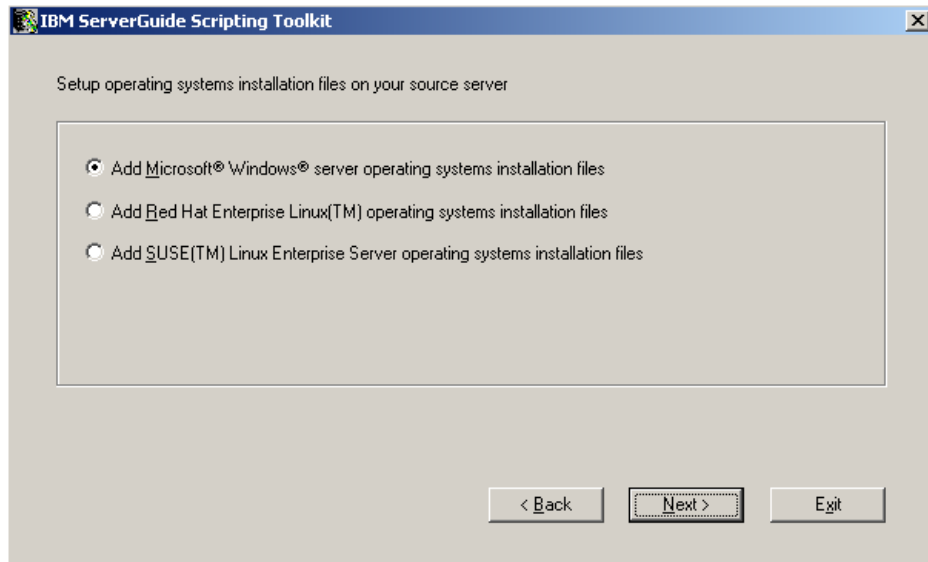


Figure 2-29 Add operating system installation files

2. If you chose Windows, another window opens giving you the option between various distributions of the Windows operating system. Select a version of Windows and make sure the correct version of the installation media is in CD-ROM drive. Click **Next**.

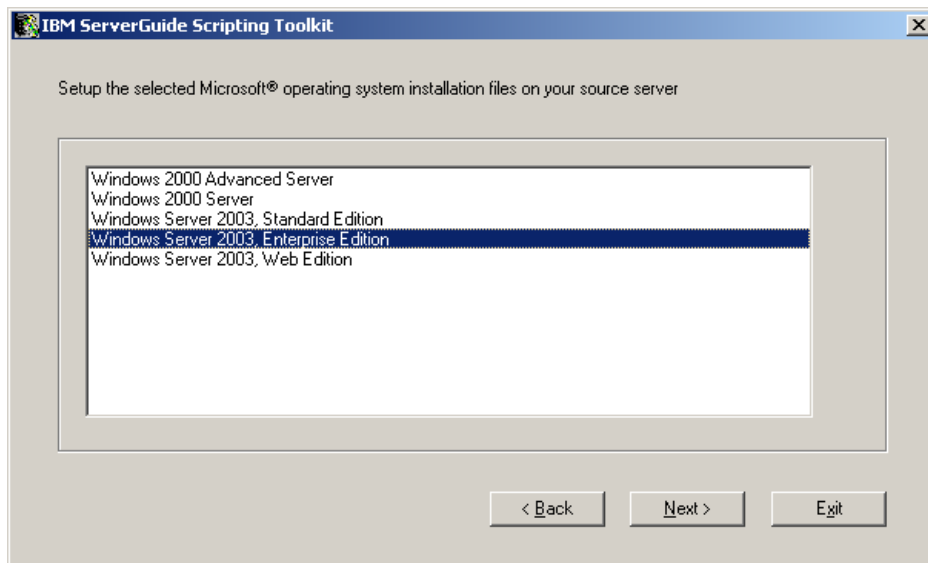


Figure 2-30 Installing operating system installation files

3. Verify that the **Source Path** text box points to the Windows install media. The **Target Folder** text box points to the folder where the I386 folder will be saved in the source tree. The default target path is highly recommended. Click **Next** to continue.

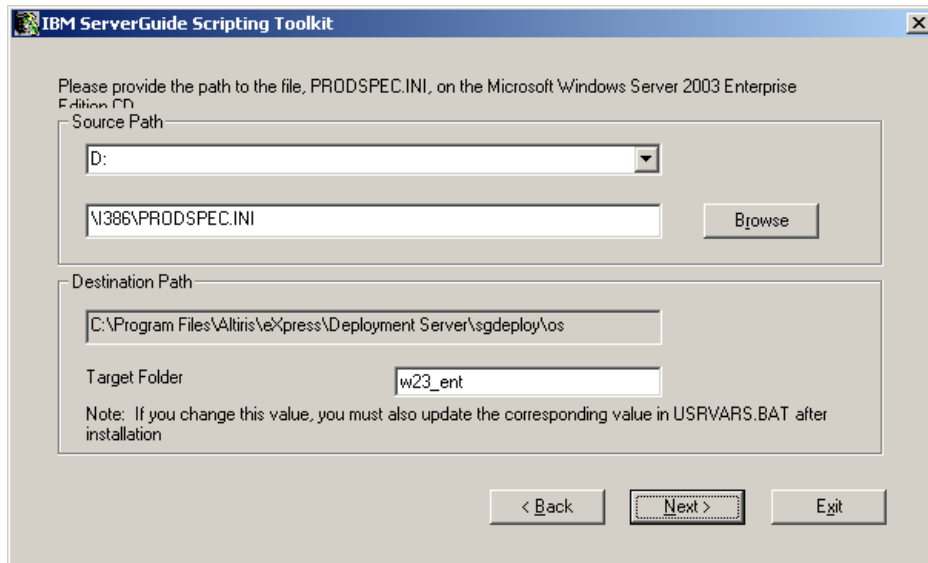


Figure 2-31 Adding operating system installation files

4. When the TKConfig window loads, click **OK** to complete the install of the Windows operating system installation files.

Add operating system utility files

Add operating system utility files as follows:

1. If you have not already done so, download the syslinux-3.11.zip from the following address and unzip it to a temporary directory:
<http://www.kernel.org/pub/linux/utils/boot/syslinux/>
2. Click **Next** to begin the install.

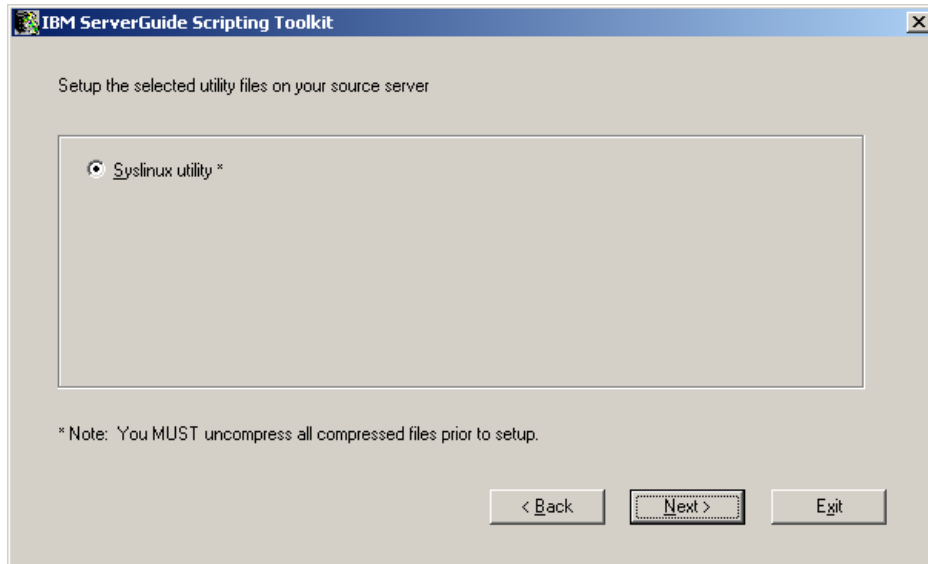


Figure 2-32 Adding operating system utility files

3. In the **Source Path** text box, specify the directory where you unpacked the syslinux zip file (locate the LOADLIN.EXE file). The variable in the Target Folder text box specifies the location in the SGTK source tree where the installation files will be saved. The default target path is highly recommended. Click **Next** to continue.

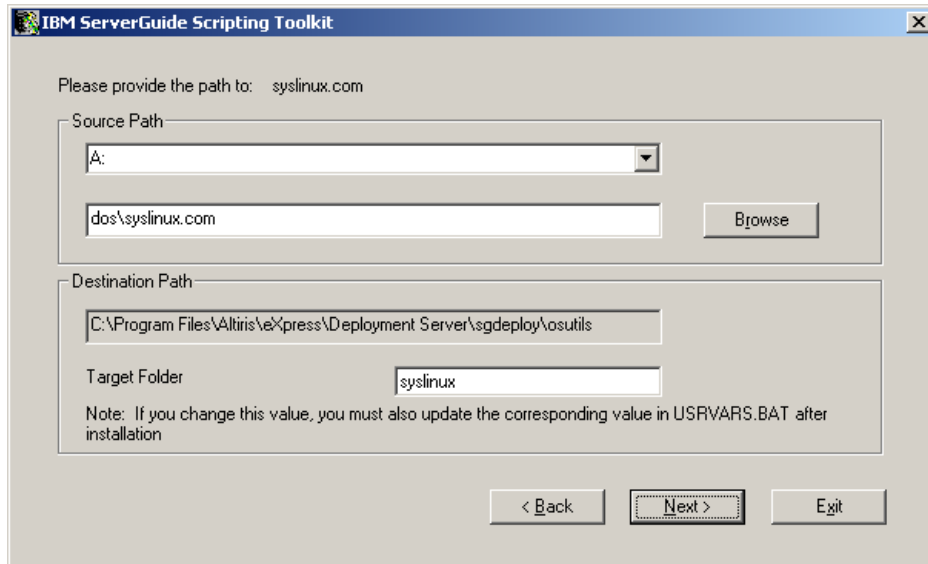


Figure 2-33 Add operating system utility files

4. When the TKConfig window loads, click **OK** to complete the install of the operating system utility files.

2.3 Installation and integration of the Deployment Agent

For the Deployment Server to be able to control a computer when it is booted into an operating system (production environment) each client computer requires the Deployment Agent (often called the *AClient*) to run as the production agent. The AClient communicates with the Deployment Server and registers the client computer in the Deployment Database. For more details on the Deployment Agent, refer to *Altiris Deployment Solution 6.5 Reference Guide*.

For Windows and Linux client systems, Deployment Solution can *push* the agent software to a client computer from the Deployment Console, or the client computer can *pull* the Deployment Agent from the Deployment Share.

Note: Altiris Deployment Solution supports all standard network adapter cards and includes many drivers. However, to avoid network card driver problems, we recommend that you check the network adapter card manufacturer's Web site for your network adaptor to make sure you use the latest driver in your pre-boot operating system configuration file.

2.3.1 Installing the Deployment Agent on Windows

The Deployment Server offers two ways of installing agent: remote install and manual install.

Remote installation of the Deployment Agent

For client computers running Microsoft Windows operating systems, Deployment Solution installs the Deployment Agent using the Remote Agent Installer to push the agent to client computers from the Deployment Console.

1. From the main menu of the Deployment Console, click **Tools** → **Remote Agent Installer** to open the utility. The first window of the Remote Agent Installer gives you the option to specify one user name and password to logon to every client computer or to specify a user name and password for each individual computer as the agent is installed. If you want to use the same password for each client (a good choice if your company has a standard user name and password) select **Use this username and password for all clients**. Enter a username in the **Username** text box, and a password for that username in the **Password** text box. Repeat the password in the field below. Click **Next** to continue.

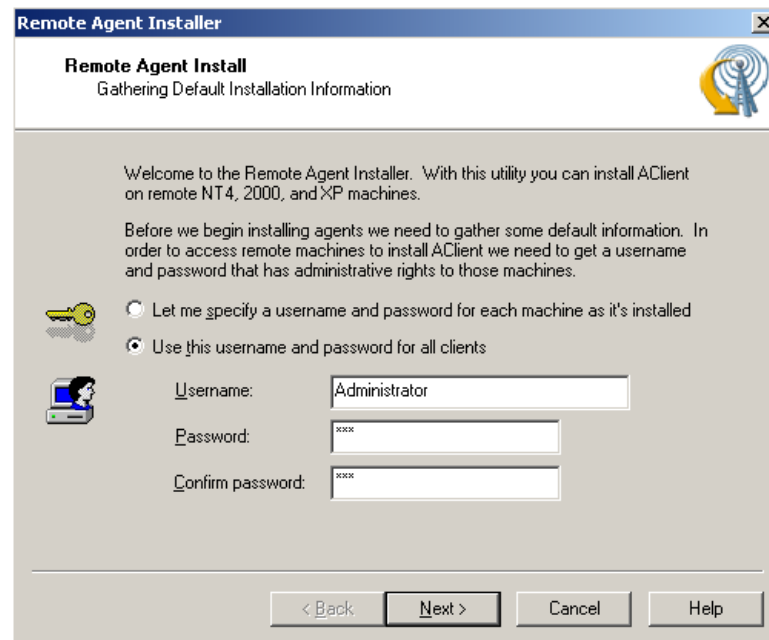


Figure 2-34 The first window of the Remote Agent Install wizard

2. When the install directory window loads, it gives you the option to change the directory on the client computer where the Deployment Agent will be installed.

Verify this path in the **Install directory** text box before continuing. Just below that field is the **Enable this agent to use SIDgen and/or Microsoft Sysprep** check box. We recommend that you enable the use of Microsoft Sysprep, so we have selected that check box. To configure the more advanced settings of the Deployment Agents that will be deployed, click **Change Settings** in the lower-right corner of the window.

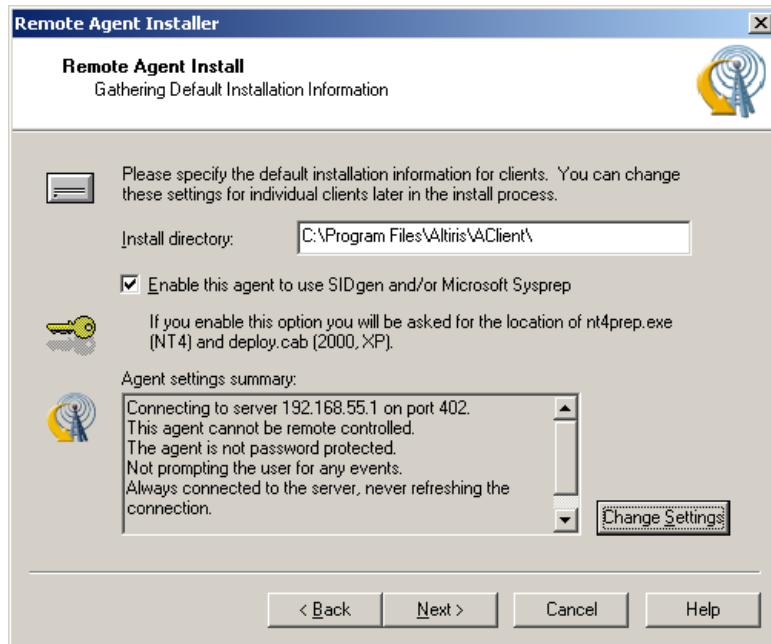


Figure 2-35 The install directory window of the Remote Agent Install wizard

3. When the Default Agent Settings window loads you will see six tabs across the top of the window. The two primary options on this tab are whether you want to have the agent contact the Deployment Server directly through its IP address, or if you would rather it use multicast using the Deployment Server's NetBIOS name and a multicast address. In our example we want the Deployment Agents to contact our Deployment Server directly so we have selected **Connect directly to this Deployment Server**. Verify the IP address and port number are correct. Click the next tab, **Access**.

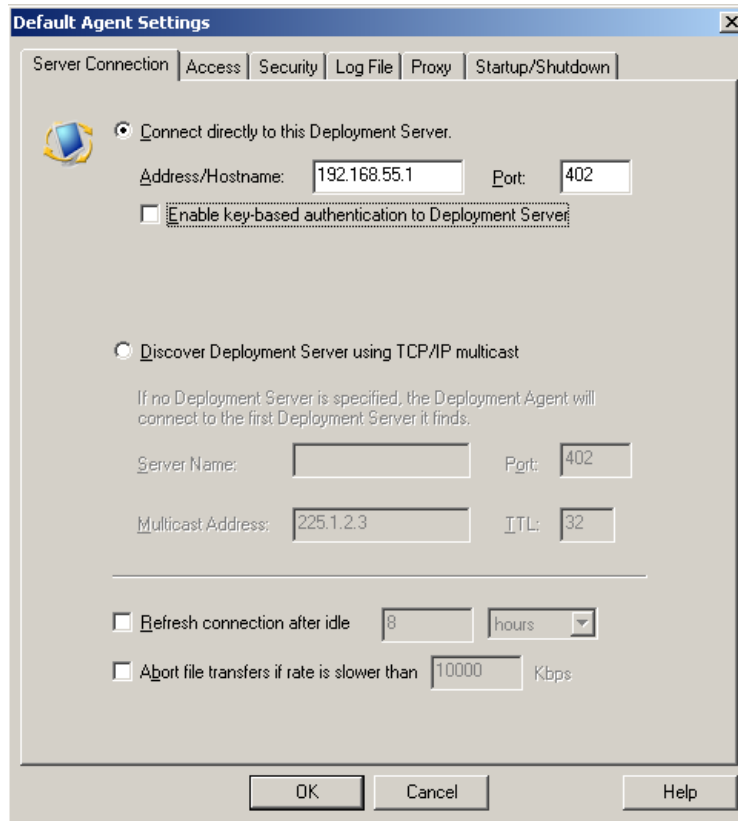


Figure 2-36 Server Connection tab of the Default Agent Settings window

4. The primary purpose of the Access tab is to limit the extent to which the Deployment Server can control the client computer. The first check box, **Allow this computer to be remote controlled**, enables/disables the ability to remote control (not unlike Microsoft's Remote Desktop) the client computer through the local Deployment Console. Although not as fluid as Microsoft's tool, the remote control function can be useful, therefore we enabled this by checking the check box.

The next three check boxes are useful when managing production computers that could possibly have someone using the computer. They enable/disable a prompt for the user when you are shutting down, restarting, copying files, or remote controlling the client computer. The **Time to wait for user response** text box specifies the number of seconds to wait for a user response before performing the action.

The next two radio buttons determine what should happen should there be no user response within the time limit specified in the text box above. You have

the option to either continue or to abort the operation. Towards the bottom of the window is a row of check boxes (one for each day of the week). Checking any of these check boxes enables two pull-down lists for entering a start time and an end time. Checking one or more of the check boxes will deny access to the client computer from the Deployment Server on the days checked during the time period specified. After making your selections click the **Security** tab.

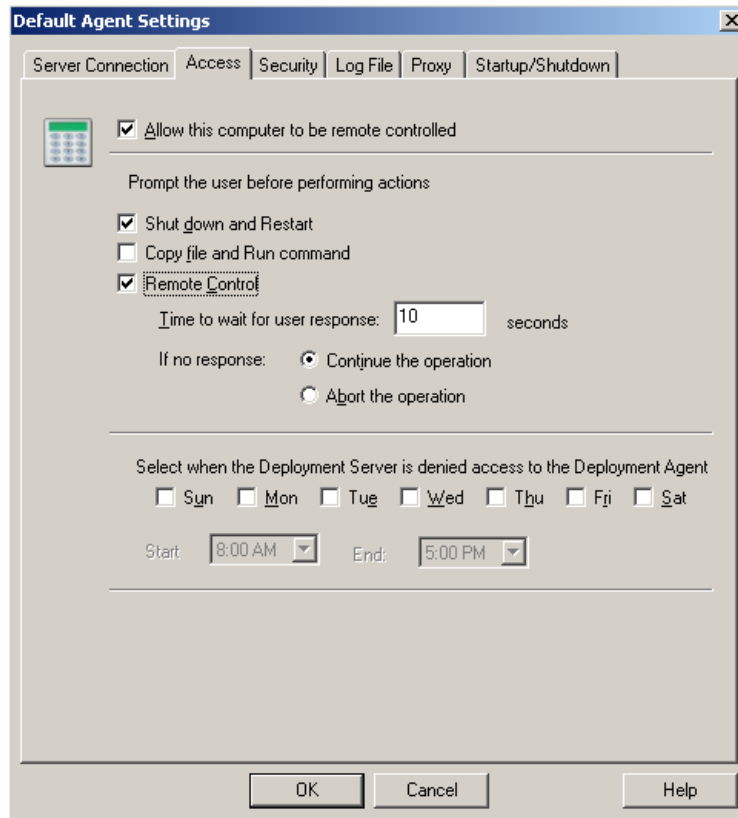


Figure 2-37 Access tab of the Default Agent Settings window

5. The purpose of the Security tab is to ensure the communication between the Deployment Agent and the Deployment Server is secure. The Security tab consists of three check boxes.

The first check box, labeled **Encrypt session communication with Deployment Server**, will stop the agent from contacting the Deployment Server unless encryption has been enabled on the Deployment Server through the Deployment Server Configuration Utility.

The second check box, labeled **Password protect Admin properties from user** controls whether a user on the client machine can change the Admin properties of the Deployment Agent. When checked, it enables two text boxes labeled **Password** and **Confirm password**. Enter a password in the first text box and then re-enter it in the second text box.

The final check box, labeled **Hide client tray icon**, enables/disables the AClient icon from showing in the client computer's task tray. The icon in the client computer's task tray can be used to shutdown the Deployment Agent. Hiding the icon makes it less likely that an end user will disable the agent. Make your selections and then click the **Log File** tab.

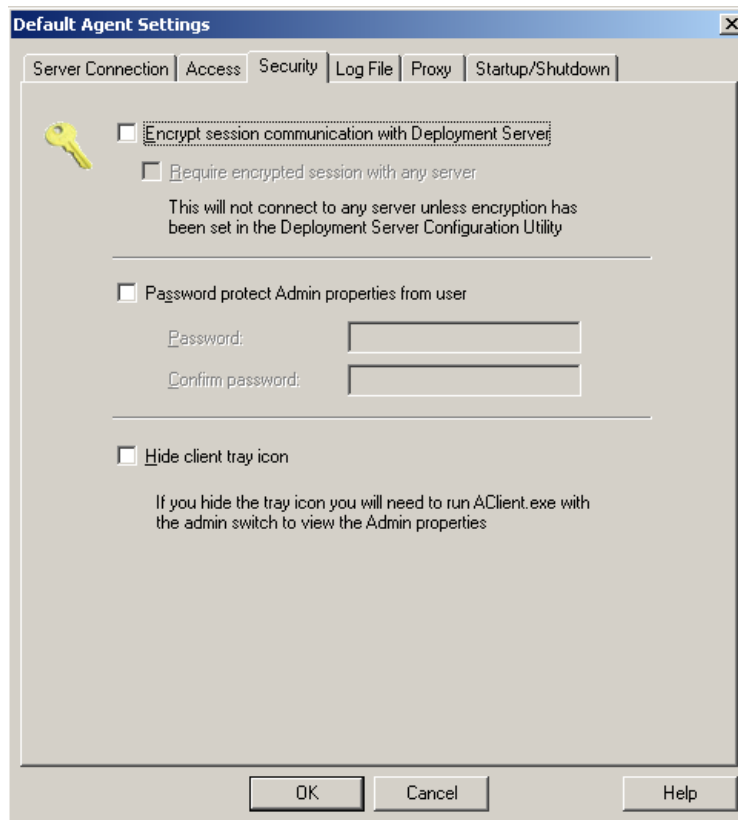


Figure 2-38 Security tab of the Default Agent Settings window

6. The Log File tab simply enables/disables a logging feature of the AClient. Checking the **Save log information to a text file** check box enables logging and enables the remaining fields on the window. The information in the **File name** text box, specifies the name of the log file and the path where it will be saved on the client computer. In the **Maximum size** text box, you can limit (in

kilobytes) the size of the log file. The three check boxes toward the bottom of the window control the data that will be recorded in the log file. Determine whether you want errors, informational messages, and/or debugging information recorded and check the corresponding check boxes. Make your selections and click the **Proxy** tab.

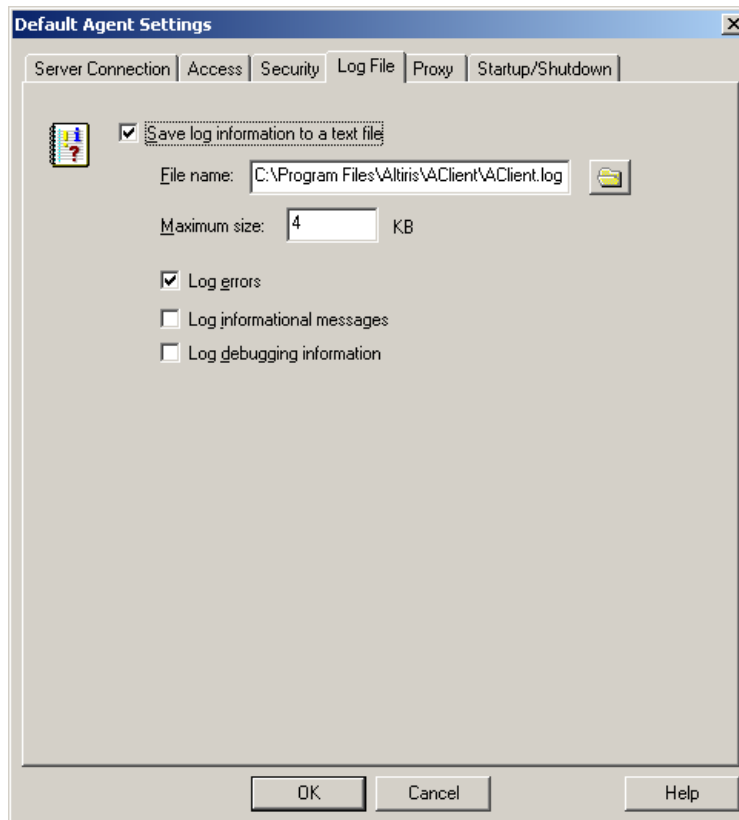


Figure 2-39 Log File tab of the Default Agent Settings window

7. The Proxy tab gives you the option to forward Wake-on-LAN packets and/or Deployment Server discovery multicast packets across multiple subnets. To enable either of these features, check their corresponding check boxes. Click the **Startup/Shutdown** tab.

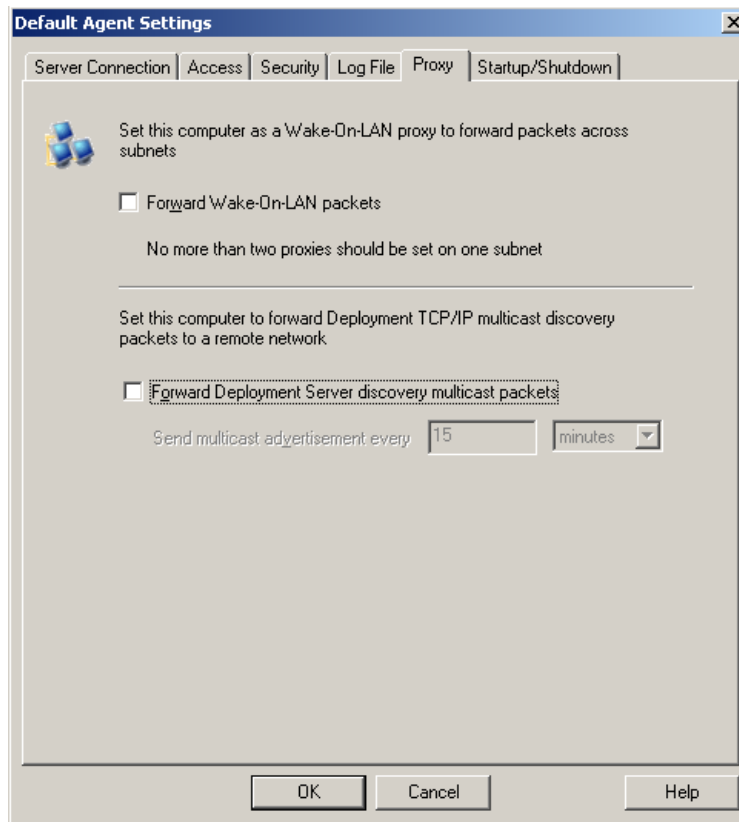


Figure 2-40 Proxy tab of the Default Agent Settings window

8. The Startup/Shutdown tab provides many options relating to the startup and shutdown of the client computer. The first text box, **Delay starting jobs after system startup**, enable you to specify a number of seconds, minutes, or hours to delay the running of any jobs that have been assigned to the client computer from the Deployment Server.

The pull-down list for **Specify the Windows boot drive** should be set to the correct letter used by Windows on the client computer. When checked, **Force all programs to close when shutting down** closes all running applications when a shutdown command has been issued to the client computer from the Deployment Server. This should be checked on computers running Windows 2003 or Windows XP.

If you want to synchronize the date and time of the client computer with that of the Deployment Server, select **Synchronize date/time with Deployment Server**.

If you want the Deployment Agent to prompt for a boot disk when performing automation jobs select **Prompt for a boot disk when performing automation jobs**. In the Advanced section of the Startup/Shutdown tab, you have the option to disable direct disk access by the Deployment Agent for DOS communication.

Select the check box in the Advanced section if you want to disable direct disk access. When you have made your selections, click **OK**. This returns you to the window shown in Figure 2-35 on page 48. Click **Next** to continue with the installation.

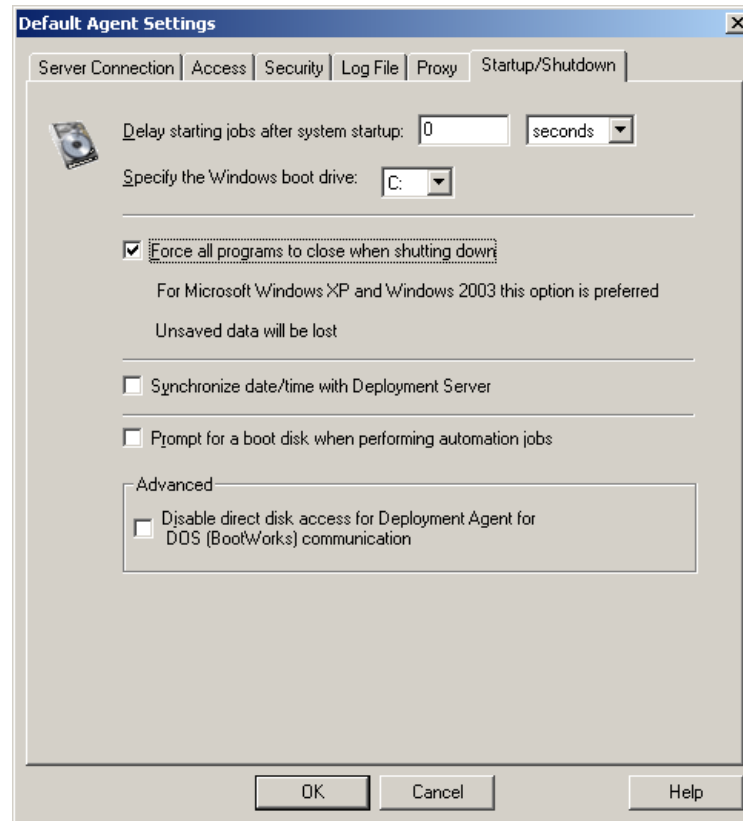


Figure 2-41 Startup/Shutdown tab of the Default Agent Settings window

9. The next window gives you the option to use the Altiris SIDgen utility, Microsoft Sysprep, or both tools when performing imaging tasks from the Deployment Console. We recommend using only the Microsoft Sysprep utility.

Do so by selecting **Use only Microsoft's Sysprep utility** from the pull-down list at the top of the window.

If you choose to use Microsoft Sysprep, the three text boxes at the bottom of the window become enabled. To use Sysprep, point the installer at the location of the Deploy.cab file, located in the following directory of your Windows installation media:

[*CDROM_Drive*]:\Support\Tools\Deploy.cab

For each Windows distribution you want to use with Microsoft Sysprep, enter the path to the Deploy.cab for that distribution. In our example we pointed to the location of the Deploy.cab file for Windows XP/2003. Click **Next** to continue.

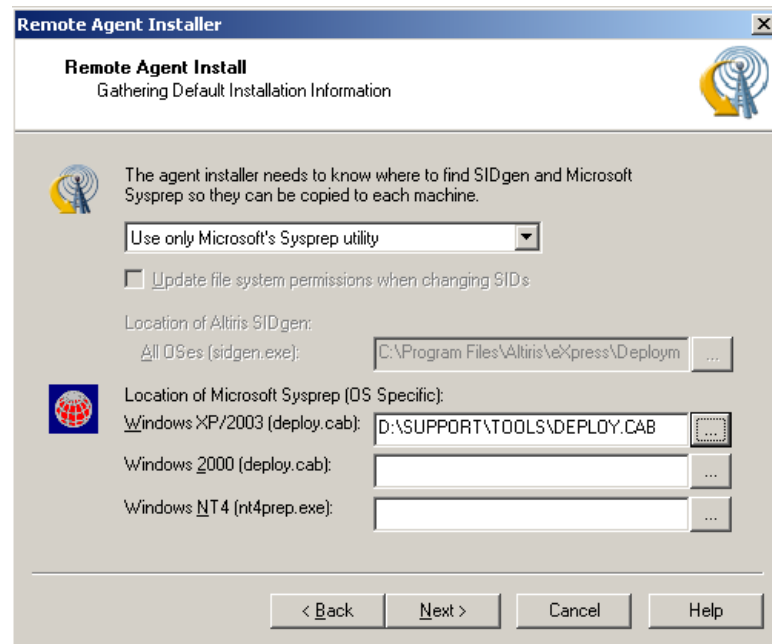


Figure 2-42 integrate Microsoft Sysprep window of the Remote Agent Installer wizard

10. On the Automatically Add to a Group window you have the option to automatically add new client computers to the default New Computers group in the Computers pane of the Deployment Console or you can specify another group in which to add the client computers. Select **Add client(s) to a default group** if you want to add them to the default group or **Add client(s) to a specific group** if you want to specify another group. If you selected the second option, you must specify the group in which to add the client computers in the text box at the bottom of the window. Click **Next** to continue.

Note: The group you specify can either be an existing group or a new group. If the group does not exist, it will be created the first time one of the client computers contacts the Deployment Server.

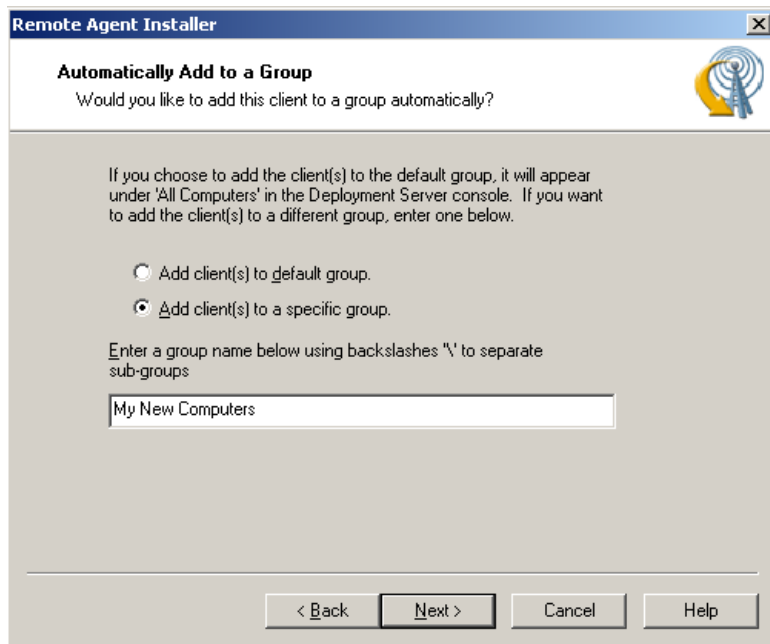


Figure 2-43 Automatically Add to a Group window of the Remote Agent Installer wizard

11. When the Selecting Clients window loads, click **Add** to create a list of clients that will be installed with the Deployment Agent. When the search window opens you can select from discovered clients or enter the IP address of a computer. Click **OK** to return to the Selecting Clients window. Click **Finish** to install the Deployment Agent to the computers listed in the Selecting Clients window.

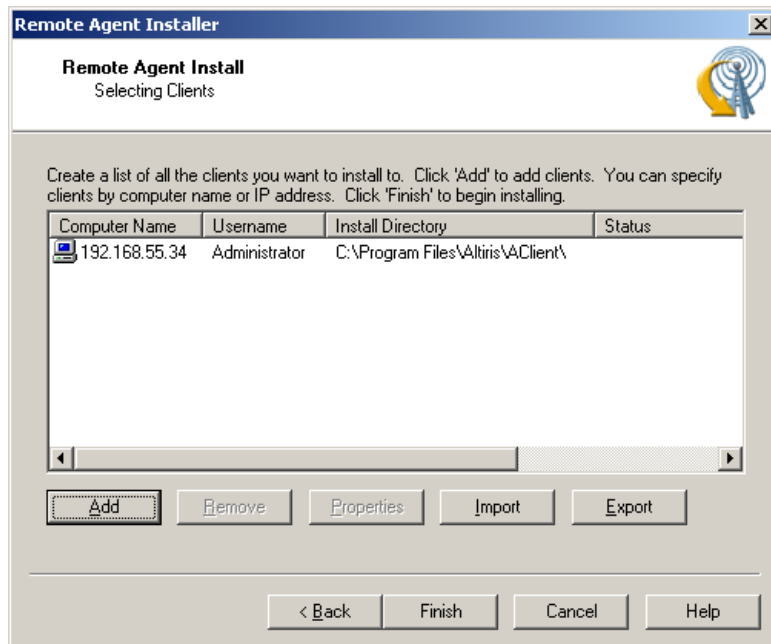


Figure 2-44 Adding client computers with the Selecting Clients window

Manual Install of the Deployment Agent

If *pushing* the Deployment Agent to your client computers will not work in your environment, you also have the option to manually install the AClient.

To perform a manual installation, access the Deployment Share on the Deployment Server from the client machine. Run the **AClient.exe** file, which can be found in directory:

\\Deployment Share\Express\Deployment Server\AClient.exe

Follow the installation as described in “Remote installation of the Deployment Agent” on page 47.

Tip: One method that could help you deploy the AClient would be to create a batch file that connects to the Deployment Share and runs the AClient.exe file. Here is the syntax for running the install using an answer file:

```
AClient.exe AClient.inp -install
```

The AClient.inp file can be edited with Notepad to customize the install for your environment.

2.3.2 Installing the Deployment Agent on Linux

Deployment Solution provides three binary files of the Deployment Agent for Linux environments:

- ▶ `altiris-adlagent-2.4-7.i386.bin` (for i386™ computers)
- ▶ `altiris-adlagent-2.4-7.ia64.bin` (for ia64 computers)
- ▶ `altiris-adlagent-2.4-7.SunOS.sparc.bin` (for computers running Sun™ OS)

To install the AClient on a Linux system, follow the steps below:

1. Determine the correct file for your environment.
2. Login to your Linux computer as the Root user.
3. Copy or download the correct BIN file (Linux installation file) from the Deployment Share to a temporary directory on the client computer.
4. From the command line on the Linux computer, drive to the temporary directory where you saved the BIN file.
5. Type **`chmod 544 filename`** to change the permission, where *filename* is the name of the installation file you downloaded.
6. Type **`.filename`** where *filename* is the name of the installation file you downloaded.

Note: The Deployment Agent will be installed in directory:
`/opt/altiris/deployment/adlagent`

7. You can change settings in the Deployment Agent configuration file (`adlagent.conf`) to match your environment by using a Linux text editor such as Vi.
8. Restart the Deployment Agent for Linux.
 - a. At the command prompt navigate to directory `/etc/rc.d/init.d` directory
 - b. At the command prompt type **`adlagent restart`**.

2.4 Communicating with Deployment Solution

Deployment Solution has the ability to perform work on a server before its normal operating system loads. To do this, the server is booted into an environment where it can communicate with your Deployment Server to perform tasks.

In Deployment Solution, this pre-boot environment is called *automation*. In order to perform image capture and deployment, scripted installs, or execute certain scripts, you must boot computers into this environment.

This section provides the information you need to choose and configure a boot method, including PXE, and select an operating environment for automation tasks. Additional sections are included containing details on the utilities provided by Deployment Server to manage these processes.

Deployment Solution uses two modes to manage computers:

Automation A pre-boot environment used primarily for imaging. Automation is also used for scripts which must be executed before a computer boots and for registry backups.

Production The normal operating system of the computer. Production tasks include software installation and personality capture.

Several of the tasks you perform can be completed in the production environment. However, other tasks, primarily imaging, must be performed before the operating system boots. In Deployment Solution, this pre-boot environment is called the automation environment, or booting into “automation mode.”

The following table contains a list of tasks and the environment in which they execute:

Note: Some of the tasks listed are only available when the IBM ServerGuide Scripting Toolkit has been installed and integrated with Deployment Solution.

Table 2-3 Tasks and the environment in which they execute

Production	Automation
Distribute Software	Capture/Deploy Disk Image
Capture/Deploy Personality	Capture/Deploy CMOS Settings
Get Inventory	Capture/Deploy RAID Settings
Copy File To	Update BIOS
Modify Configuration	Scripted OS Install
Power Control	Update RAID Controller BIOS/Firmware
Run Script	Run Script
	Backup/Restore Registry

In order to manage computers in a pre-boot state, you must select a method to boot computers to automation, then decide which operating system to use in the automation environment.

Deployment Solution provides support for a broad range of boot methods and automation operating systems; this section helps you decide which works best for your environment.

In order to set up automation, you must make the following decisions:

- ▶ Which pre-boot operating system do you want to use?
- ▶ Which automation boot method works best for your environment?

We discuss these in the following sections.

2.4.1 Which pre-boot operating system do you want to use?

Deployment Solution supports the following automation operating systems: Windows PE, Fedora Linux, MS-DOS, and FreeDOS. This section provides an overview of the available automation operating systems, so you can find an environment (or environments) that suits your needs.

An important thing to note is that the automation environment you use is not constrained by the production operating system on the computer. All of the Deployment Solution automation tools support these operating systems, so you can perform automation tasks in any operating system (Linux computers can be imaged from DOS, Windows computers can be imaged from Linux, and so on).

You might even use two automation operating systems for different tasks within the same job. For example, you might perform a BIOS update in DOS, then boot to Windows PE or Linux to perform an imaging task.

When you set up your test environment, you might want to run automation jobs in multiple operating systems to see if one performs better in your environment.

The following sections give a brief overview of the automation operating systems.

DOS

DOS is still used often today as a pre-boot environment, though new technologies have emerged that might better suit your environment, such as Windows PE.

The largest roadblocks most companies face when using DOS are access to drivers that support modern hardware, and security concerns. DOS still performs well for several tasks though, and can be a good choice if you have the proper driver support.

DOS typically requires only around 1 MB of space.

DOS provides an additional advantage in a PXE environment. When performing an automation task on multiple computers, the PXE server can use multicast to boot automation, which enables large numbers of managed computers to boot DOS simultaneously.

Windows PE

Windows PE (Windows Pre-boot Environment) is the next generation boot environment for Windows computers. Windows PE provides several advantages over DOS, including better driver support (Windows PE uses the same drivers used by the other modern versions of Windows), increased speed, and generally more functionality.

Windows PE typically requires around 150 MB of space.

The biggest drawbacks are its size, which causes increased boot time, especially when booting over the network using PXE, and its licensing requirements. Additionally, clients using Windows PE require at least 256 MB of RAM. In addition to its size, Windows PE also does not support multicast.

Fedora Linux

Fedora Linux provides an alternate pre-boot environment to DOS or Windows PE. The Fedora distribution used by Deployment Solution includes the 2.6.11 Core 3 kernel and a number of network drivers supported by this kernel. Additional drivers can be compiled against this kernel and added as well. Many vendors provide Gigabit Ethernet and wireless drivers for Linux that are not available in DOS.

Linux typically requires around 10 MB of space.

Linux can be a good choice if you do not want to license MS DOS or Windows PE, but you need updated driver support.

2.4.2 Which automation boot method works best?

After you have determined which operating systems you want to use in the automation environment, you need to determine how to boot your client computers into automation. Again, Deployment Solution supports a broad range of environments: PXE, automation partitions, or boot media (CD, USB device, or diskette).

This section provides an overview of the available boot methods to help you select the method that works best for your environment, and contains the following:

- ▶ PXE
- ▶ Automation Partitions
- ▶ Boot Media (CD, USB Device, Floppy)

PXE

Pre-boot Execution Environment (PXE) is an industry standard developed to boot computers using a network card. PXE can boot computers regardless of the disk configuration or operating system installed, and doesn't require any files or configuration settings on the client. After PXE boot is turned on in the system BIOS, a computer can communicate with your PXE Server to receive automation jobs.

PXE provides a number of advantages, especially when you are using the initial deployment features of Deployment Solution, which enables you to remotely deploy an image to a computer which has no software installed.

For example, the receiving department of your company could have PXE enabled on their subnet. When a new computer arrives, a technician could quickly unpack and plug the computer into the network, power on the computer, and enable PXE boot in BIOS (if it was not enabled by the manufacturer). When this unknown computer contacts the Deployment Server, it is assigned an initial deployment job, which could image the computer with the corporate standard image, install additional packages, then power off the computer. The computer is now ready for delivery with minimal effort.

PXE also provides an advantage if you need to use multiple automation operating systems in your environment. Since the image containing the automation operating system is downloaded when a task is executed, different operating system environments can easily be assigned to different tasks.

At the same time however, this can be a disadvantage if you are using an operating system with a large footprint, such as Windows PE, since the entire image must be downloaded each time you run an automation task. If you often run automation jobs, especially on several computers simultaneously, embedding the automation operating system on the disk is faster and significantly reduces network traffic.

It is also possible to use PXE for initial deployment, then install an automation partition as part of the deployment. In this case, you could use the initial deployment features of PXE for arriving computers, then install an automation partition in case you need access to automation at a later time.

This configuration does not require PXE in your general network environment, but still provides access to the automation environment without physical access.

When using the DOS automation environment, PXE provides an additional advantage: multicast boot. This enables your PXE server to simultaneously boot up to 100 computers in a single session to perform automation work. PXE multicast booting is not provided by Windows PE, and is not supported on Linux.

Images can still be deployed using multicast to all supported automation environments, but non- DOS operating systems must be booted using unicast, which is considerably slower.

Using PXE as a boot option is recommended, and is covered more thoroughly in 2.5, “Configuring and using PXE pre-boot environment” on page 64.

Automation partitions

An automation partition is a sector of your hard disk drive partitioned and managed by Deployment Solution. This partition contains the automation operating system and the files needed to contact your Deployment Server, and must be present on each managed computer.

The biggest advantage to an embedded partition is that it does not require PXE, yet it still enables you to boot into automation remotely. The biggest disadvantages to embedded partitions is that they consume space on the drive, they requires an existing partition on the drive, and they must be manually installed from a disk on Linux and UNIX operating systems.

Another drawback, depending on your configuration, might be the fact that only one automation operating system can be installed to a managed computer that is using an automation partition. If you have tools that are supported only in DOS, this might limit you to DOS for all automation tasks on a particular managed computer.

Automation partitions have an additional advantage in some configurations. Optionally, you can create a different type of automation partition, called a hidden partition, to store an image (or other files) locally.

This provides advantages in environments where computers need to be re-imaged often, or in environments where there is limited bandwidth or network connectivity. Since the image is stored locally, the time needed to create and restore images is greatly reduced and network traffic is significantly reduced as well.

Automation partitions are not covered in this document. However, if you want to learn more, reference the *Altiris Deployment Solution 6.5 Reference Guide*. This document can be found at the following URL:

<http://www.altiris.com/Support/Documentation.aspx>

Boot Media (CD, USB device, diskette)

Generally, the biggest drawback to boot media is that it forces you (or someone else) to physically access the computer. However, if you are managing smaller numbers of computers, or do not plan to access the automation environment

often, it might be a good choice. Also, if you have employees with the ability and access to boot their own computers using disks you provide, this could also be a good solution.

Boot media has some configuration limitations though. Deployment Solution is designed to manage computers remotely, even in the automation mode, and several tasks and jobs require access to both the production operating system and the automation environment (for example, an imaging operation first captures configuration details from the production operating system before booting to automation to capture the image).

Because of this, it is often difficult to schedule a job, then coordinate booting the managed computer to the right environment at the right time. If you assign a job which requires booting into automation mode, the boot disk must be present at the right time to boot automation. If a complex job requires access to the production environment during this time, the BIOS will most likely continue to boot to automation until the boot media is removed. If this job, or a subsequent job, requires automation access again, the boot media must be re-inserted.

To avoid these issues, some customers load the Deployment Solution tools, the RapiDeploy imaging executable, and the image on physical media. They then boot a computer, execute the necessary commands, then provide the required image files. In this circumstance, the remote management capabilities of Deployment Solution are not being used, so the process is more manual, but it does not require network access.

This works especially well when managing thin clients or other computers where all necessary files can fit on a single disk or USB device.

Boot media is not covered in this document. However, if you want to read more, read the *Altiris Deployment Solution 6.5 Reference Guide*. This document can be found at the following URL:

<http://www.altiris.com/Support/Documentation.aspx>

2.5 Configuring and using PXE pre-boot environment

PXE is the recommended automation boot method. It allows for remote management of client computers and does not require touching the computers.

To fully utilize the PXE pre-boot environment a number of steps are required:

- ▶ Determine the number of PXE Servers required
- ▶ Install a DHCP server with an active scope
- ▶ Configure the client computer to boot from the network

- ▶ Place the client computer, the Deployment Server, and the DHCP server on the same subnet (it is possible to utilize Deployment Solution in multiple subnet environments. See 2.5.4, “Using the PXE across multiple subnets” on page 68 for more information.

The following sections will cover these areas in more detail.

2.5.1 Determining the number of PXE servers you need

When determining the number of PXE servers required to meet your needs, a number of factors should be considered:

- ▶ The number of clients that will be connecting to the PXE Server simultaneously
- ▶ The speed of your network infrastructure
- ▶ The type of PXE pre-boot operating system you will be using (for example, WinPE or DOS)
- ▶ The physical layout of your network

Number of client connections

PXE Servers do not typically require a lot of resources. By using multicast, a single PXE Server can deploy a boot image to up to 100 computers at a time, and not consume any more resources than it would deploying a single image. Multiple multicast sessions can be executed simultaneously.

If you are going to be imaging more than 100 computers additional PXE Servers can easily be added.

Note: In most cases a single PXE Server is adequate and recommended for simplicity.

Network speed

Since the majority of the resources on the PXE Server are used transferring files over the wire, the faster the network, the more work a single PXE Server can do. A single PXE Server on a gigabit network can remotely boot a larger number of computers over a period of time than even multiple PXE Servers on a slower network.

This becomes especially important when using certain automation environments, such as Windows PE, that can be over 100 MB and do not provide support for multicast booting. Boot files must be delivered to each of these managed computers individually, causing a large amount of network traffic and greatly increased boot times.

This is less of an issue when using boot images with a small footprint, such as DOS, which support multicast booting.

Physical layout of your network

A PXE deployment is often set up according to the physical layout of your network. If you have three offices in different locations, it might make sense to install a PXE server at each location to reduce traffic and resolve routing issues.

In these configurations, the Deployment Share can be mirrored to a local server, and images are usually taken from and restored to local file servers.

2.5.2 Enabling network boot on the client computer

To utilize the PXE pre-boot environment, the client computer must be enabled to boot from the network before it boots from the hard disk.

Tip: IBM computers have the option to select the boot device during POST (F12). This is a one time only boot (e.g. the computer reverts to its normal boot routine the next reboot). Some jobs or tasks that are assigned from the Deployment Server require more than one reboot. If F12 is used to boot from the network, the Deployment Server could lose control of the computer if the job requires more than one reboot causing the job or task to fail. It is a best practice to permanently change the boot order of the computer to boot from the network before the hard disk.

Perform the following steps to enable network boot on the client computer:

1. Power on the client computer.
2. When prompted, press F1 to enter the BIOS Setup menu.
3. In the BIOS menu, scroll down to **Startup Options** and press the Enter key.
4. Highlight **Startup Sequence Options** and press the Enter key.
5. Re-order the primary startup sequence so network is the first boot option, or at least before the hard disk. (For example: Network, Diskette Drive 0, CD ROM, Hard Disk 0)

Note: Some computers have the option to enable or disable PXE on certain network interface cards (NICs). Verify that PXE is enabled for the NIC you plan to use if your computer's BIOS supports this function.

6. Exit Setup and save changes when prompted. The computer will reboot.

2.5.3 Connecting to the Deployment Server using PXE

When the client computer has been configured to boot from the network, it uses PXE to connect to the Deployment Server.

Before connecting to the Deployment Server verify the items listed below:

- ▶ Your client computer is physically connected to the network and is on the same subnet as your DHCP server and your Deployment Server (for suggestions on using PXE across multiple subnets see 2.5.4, “Using the PXE across multiple subnets” on page 68).

Note: It is a best practice to use NIC port 0 when using PXE unless you are using a feature called Serial Over LAN. If you use NIC port 1 it is possible to miss the DHCP offer, skipping PXE. Some System x systems have a feature called Serial Over LAN that uses NIC port 0 and needs to have PXE disabled on that port.

- ▶ Your DHCP server is active (with a scope defined) and on the same subnet as your client computer and Deployment Server.

When you have verified the configuration you are ready to connect to the Deployment Server.

Follow the steps outlined below to connect:

1. Power on the client computer.
2. If your computer and network have been configured properly, the computer will boot to the network and get a DHCP offer from the DHCP server.
3. When the PXE boot menu appears, select one of the options and press the **Enter** key to initiate the connection (**DOS Managed** is the default MS-DOS PXE boot image that is created if you loaded the MS-DOS files during the install of Deployment Solution).

Note: If the client computer is currently a managed computer (it has a record in the Deployment Database and has a corresponding icon in the Computers pane of the Deployment Console) the computer will PXE boot and then immediately boot to production. To force the computer to stop at the PXE boot menu, go to the Deployment Console right-click its icon in the Computers pane and select **Delete** from the context-sensitive menu to remove the computer’s record from the Deployment Database.

When connected, the Altiris PXE Server will download a PXE boot image to your client computer. When the client computer displays the following message, you are connected to the Deployment Server and ready to assign jobs:

The deployment server has instructed Bootworks to wait.

Note: For environments where PXE cannot be used, Altiris offers technologies such as BootWorks that can be used in place of the Altiris PXE Server. Although Altiris BootWorks does not provide the same level of hands-free management that PXE offers, it is a reasonable alternative in many environments. For more information regarding optional connection methods, refer to *Altiris Deployment Solution 6.5 Reference Guide*.

2.5.4 Using the PXE across multiple subnets

There are a couple methods for using PXE across multiple subnets:

- ▶ Enabling broadcast and multicast packet forwarding on your routers
- ▶ Installing multiple PXE Servers (one in each subnet)

PXE Request Routing

Client computers use broadcast packets to find DHCP and PXE services on a network, and multicast packets (MTFTP) to transfer files. These packet types can present challenges when planning a PXE deployment because most default router configurations do not forward broadcast and multicast traffic.

To resolve this, either your routers need to be configured to forward these broadcast and multicast packets to the correct server (or servers), or you need to install a PXE Server on each subnet.

Routers generally forward broadcast traffic to specific computers. The source subnet experiences the broadcast, but any forwarded broadcast traffic targets specific computers.

Enabling a router to support DHCP is common. If both PXE and DHCP services are located on the same computer, and DHCP packet forwarding is enabled, you shouldn't have any problem transferring broadcast packets.

If these services are located on different computers, additional configuration might be required.

If you are going to forward packets, make sure your router configuration allows DHCP traffic to access the proper ports and IP addresses for both DHCP and PXE servers.

When the broadcast issues are resolved, the routing of multicast traffic must be considered. Multicasting leverages significant efficiencies in transferring files but also introduces challenges similar to broadcast packet forwarding. Like the broadcasting solution, routers can be configured to support multicast traffic between client computers and the PXE Server.

Please consult the documentation provided by your router vendor for additional information about packet forwarding.

Installing additional PXE Servers

After you have determined the PXE needs of your network, you must to determine where to install the additional PXE Servers.

A PXE Server can be installed on your Deployment Server, on your DHCP server, on another server in your network (such as a file server), or as a standalone server. You can also use a combination of these (for example, a PXE server on your Deployment Server and your DHCP server).

The actual installation process is straightforward. You can install a PXE Server at the same time as you install Deployment Solution, or you can install one later by running the installation program again from your Deployment Server and selecting the add additional components option. See 2.1.5, “Component installation” on page 25 for more information about the installation process.

After these servers are installed and running, they are configured using the PXE Configuration Utility, which is found by opening the Deployment Console and clicking **Tools** → **PXE Configuration Utility** from the main menu. The PXE Configuration Utility is covered in depth in the *Altiris Deployment Solution 6.5 Reference Guide*. This document can be found at the following URL:

<http://www.altiris.com/Support/Documentation.aspx>

2.6 Integrating with the IBM Service Processor Discovery utility

The IBM Service Processor Discovery utility gives the Deployment Solution the ability to remotely manage the power of computers via the power management features of the following service processors:

- ▶ IBM BladeCenter Management Module
- ▶ IBM Remote Supervisor Adapter
- ▶ IBM Remote Supervisor Adapter II (RSA II)

This utility, when integrated with Deployment Server, allows the user to discover, enter, modify, and delete service processor information of IBM System x Servers and the IBM BladeCenter Management Module. When a service processor/management module is discovered, the utility will expose new functionality in the right-click menu of a managed computer in the Computers pane of the Deployment Console. The following new features are available in the right-click menu when clicking on a managed computer in the Computers pane of the Deployment Console for computers that have associated records in the `service_processor` table in the Deployment Database:

- ▶ Power on the server
- ▶ Power off the server
- ▶ Launch the Web interface of the service processor/management module

The IBM Discovery Utility leverages the IBM Management Processor Command Line interface (MPCLI) to perform these functions.

Without this additional power control, Deployment Solution is only able to control power through Wake-on-LAN and the operating system's shutdown/power off calls (ACPI). The power off feature will do an immediate power off of the server using the service processor.

The IBM MM/RSA/RSAII Interface menu option will launch a Web browser and automatically load `http://ipaddress` where *ipaddress* is the host name field found in `service_processor` table in the Deployment Database.

2.6.1 Configuring the IBM Service Processor Discovery utility

The IBM Service Processor Discovery utility installer is a MSI file that is copied into the Deployment Share during the Deployment Solution installation.

Note: When the ServerGuide Scripting Toolkit versions 1.3.02 and later are installed and integrated with Deployment Solution, the SGTK installer will detect and automatically install the IBM Service Processor Discovery utility without any operator intervention.

To install and configure the IBM Service Processor Discovery utility follow the steps outlined below:

1. Close the Deployment Console.
2. From the root folder of the Deployment Share (default is `c:\Program Files\Altiris\Express\Deployment Server`), run the `ibmtools.msi` setup file. This will install the IBM Service Processor Discovery utility.

3. Download and install the management processor command line interface (MPCLI) tool, which can be found at the following URL:
<http://www.pc.ibm.com/support?page=MIGR-54216>
4. Open the Deployment Console.
5. Verify that the Blade or System x computer you want to manage is displayed and shown as active in the Computers pane of the Deployment Console.
6. From the Deployment Console's main menu, click **Tools** → **IBM Tools** → **IBM Service Processor Discovery**. This will start the utility as shown in Figure 2-45.

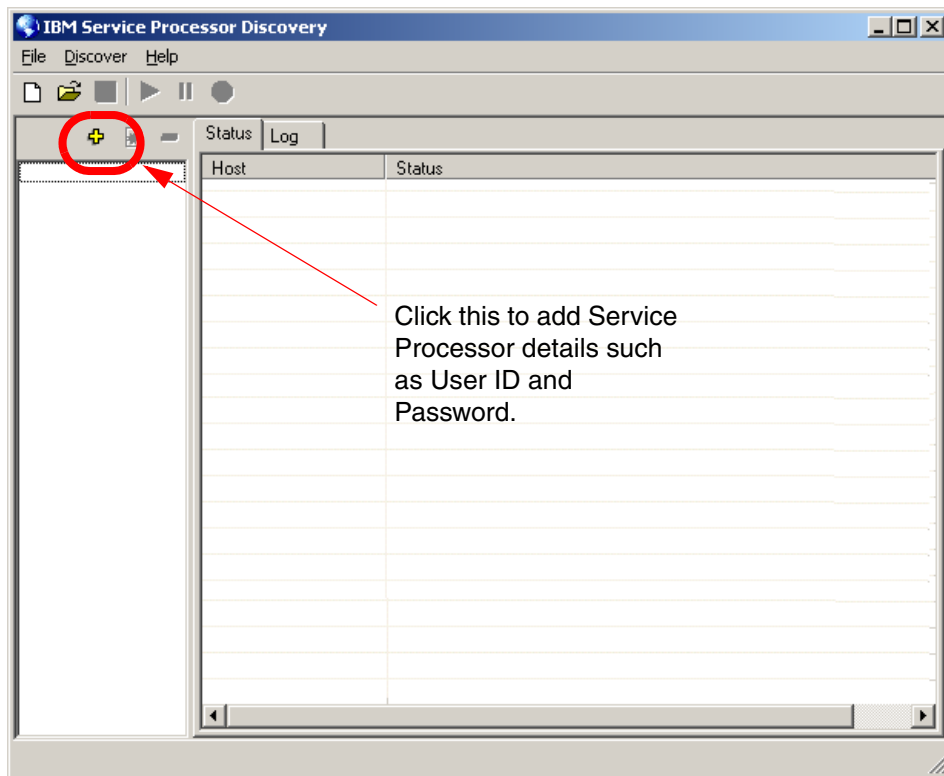



Figure 2-45 The Service Processor Discovery utility

7. Next we need to add the service processor details to the Deployment Database. Click the  shown above to open the Discovery Group window shown in Figure 2-46 on page 72.

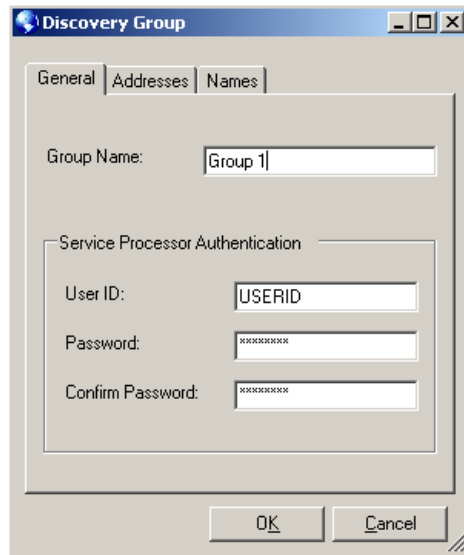


Figure 2-46 Enter a Group Name, User ID, and Password for the service processor

8. On the General tab of the Discovery Group window, enter a unique text string for the Group Name, and the User ID and Password of the computer's service processor (or if you are using an IBM BladeCenter enter the User ID and Password for the enclosure's management module).

Tip: The Group Name can be anything unique. It is not used outside this utility.

9. Click the **Addresses** tab to specify a range of IP addresses to search or click the **Names** tab and enter the host name or IP address of the service processor or BladeCenter enclosure's management module.

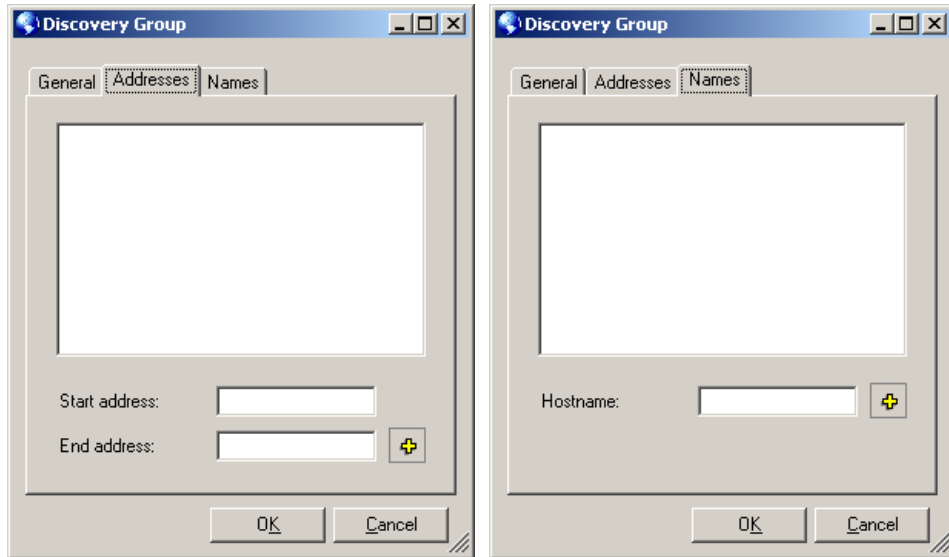


Figure 2-47 Enter the host name of the service processor or an IP address range to search

10. Click **OK** to close the Discovery Group window and save the information you entered.
11. Start the discovery process by highlighting a group in the left pane and clicking the **Play** icon. You will see something similar to Figure 2-48 on page 74.

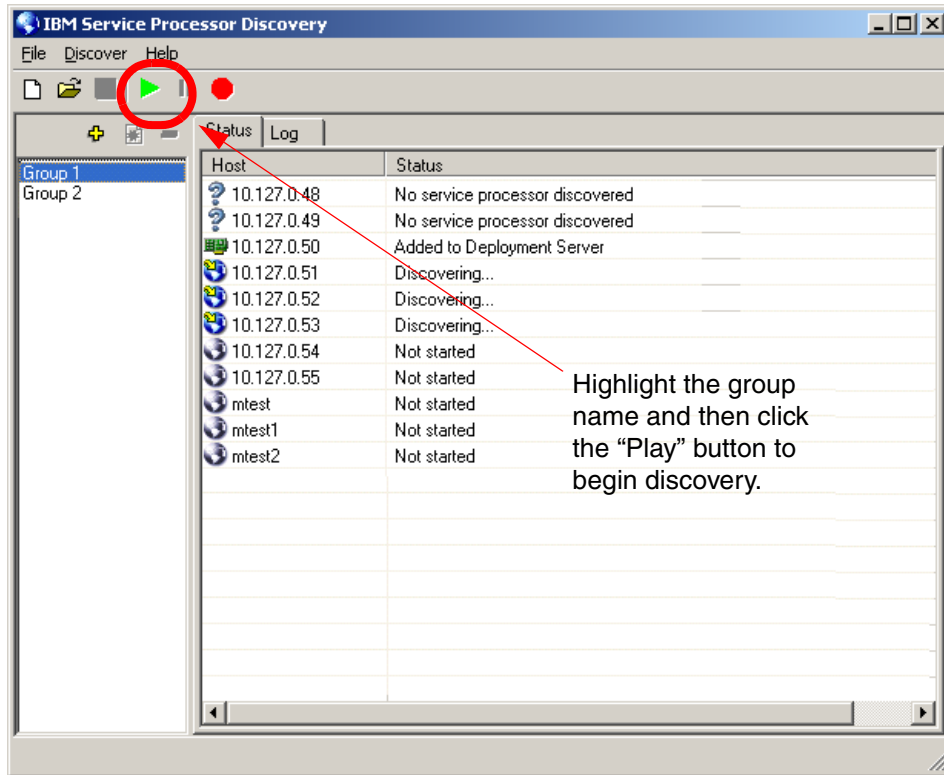


Figure 2-48 The IBM Service Processor Discovery utility discovering service processors

Note: The discovery process uses the MPCLI you installed earlier. If you did not install it, you will be prompted to install the utility now.

When a service processor has been found, it will be entered into the Deployment Database.

12. Close the discovery tool to return to the Deployment Console.
13. Right-click a managed computer in the Computers pane of the Deployment Console that has a service processor you just discovered installed and expand the **Power Control** task in the context-sensitive menu. You should see options for performing power control through the service processor at the bottom of the expanded menu.

2.7 Best practices

In this section, we share several best practices to better utilize Deployment Solution.

2.7.1 Create a backup of sample jobs

We recommend making a backup copy of the sample jobs that are included with the integration of the ServerGuide Scripting Toolkit in the Jobs pane of the Deployment Console before any customizing of the jobs takes place. This way the original jobs will still be available as a reference if your production jobs need troubleshooting.

To copy jobs in the Deployment Console follow the steps outlined below:

1. In the Jobs pane of the Deployment Console, right-click the folder you want to copy.
2. Select **Copy** from the right-click menu.
3. Right-click any open space within the Jobs pan, and select **Paste** from the right-click menu.
4. Rename the new folder to fit your production needs.

2.7.2 Set PXE to use Ethernet port 0 rather than port 1

Deployment Solution uses two modes to manage systems: automation and production.

- ▶ Automation is a pre-boot execution environment (PXE) used primarily for imaging. Automation is also used for scripts which must be executed before a computer boots and for registry backups.
- ▶ Production is the normal operating system of the computer. Production tasks include software installation/distribution and setting captures.

Several tasks must be executed before the operating system boots. This pre-boot environment is called automation environment, or booting into automation mode.

PXE uses standard network protocols such as TCP/IP to establish a communication channel between a computer and a PXE server during the boot process. Using this channel, a PXE server sends an execution environment to the computer so that work can be performed in a pre-boot state. All tasks defined in ServerGuide Scripting Toolkit can be executed in this environment.

How you implement PXE depends on what you plan to do with it. For example, for network security reasons, many large organizations use PXE only on a

designated subnet in a receiving end to deploy corporate images, initial configuration, layered software such as anti virus, backup and monitoring agent, and quality assurance. After this computer is rolled into production, PXE is not used in normal production environment any more.

PXE boot to Ethernet port 0 versus 1

PXE usually boots to first network interface port, port 0. Depending on how you use the ports, you can set first port for PXE boot with DHCP and second port for production subnet. You can modify protocol.ini file in the /net folder on the boot disk to fit your needs.

Serial over LAN

When Serial over LAN (SOL) is enabled, port 0 will not be available for PXE boot. You must modify protocol.ini to use other available ports.

2.7.3 Change the primary lookup key to Serial Number

The primary lookup key specifies the lookup key type used to associate a new computer contacting the Deployment Server with a managed computer already existing in the Deployment Database. The options are Serial Number (SMBIOS), Asset Tag (SMBIOS), UUID (SMBIOS) or MAC Address. MAC Address is the default. However, if MAC address is used and the client computer has two NICs the identity will switch between the first and then the second NIC as each connects to the Deployment Server. This could cause additional reboots and potential issues with the assignment of jobs and other tasks. The best practice is to set the primary lookup key to use the serial number of the client computer rather than the MAC address.

Change the primary lookup key by following the steps outlined below:

1. From the main menu of the Deployment Console, click **Tools** → **Options** and then select the **Global** tab.
2. Toward the bottom of the tab there is a pull-down list labeled **Primary key lookup**. Select **Serial Number (SMBIOS)** from the options given.

2.7.4 Synchronize the display names with NetBIOS computer name

It is good idea to synchronize the computer's NetBIOS name with the name that is displayed on the Deployment Console for ease of management, especially in large organizations.

Synchronize the display names by following the steps outlined below:

1. On the Deployment Console, click **Tools** → **Options** and select the **Global** tab.
2. Check **Synchronize display names with Windows computer names**.



Scenarios

This chapter explores the possible scenarios of deployment for your organization. Also common issues are provided for your planning reference.

The following topics are covered:

- ▶ 3.1, “Initial deployment” on page 80
- ▶ 3.2, “Pre-staging computers for deployment” on page 89
- ▶ 3.3, “Linking multiple deployment jobs together” on page 93
- ▶ 3.4, “Job troubleshooting” on page 96
- ▶ 3.5, “Common issues” on page 99

3.1 Initial deployment

Initial Deployment is a default job designed to aid in the process of setting up computers that do not have existing records in the Deployment Database. Initial Deployment allows you to define how computers are initially set up after being powered on and have contacted the Deployment Server.

Note: Initial Deployment is ideal for small scale deployment (1 to 14 computers). For larger deployments, you should consider using virtual computers, customized jobs and the computer import feature. See 3.2, “Pre-staging computers for deployment” on page 89.

This section describes the properties of Initial Deployment jobs. In the Jobs pane of the Deployment Console, double-click the **Initial Deployment** job to load the Properties of Initial Deployment window. As shown in Figure 3-1 on page 81, there are three tabs: Configurations, Jobs, and Advanced.

3.1.1 Configurations tab

The Configurations tab allows you create a menu of profiles that each contain a set of configured computer properties. This menu will be presented to the user when the Initial Deployment job is executed allowing the user to select which profile to apply to the computers.

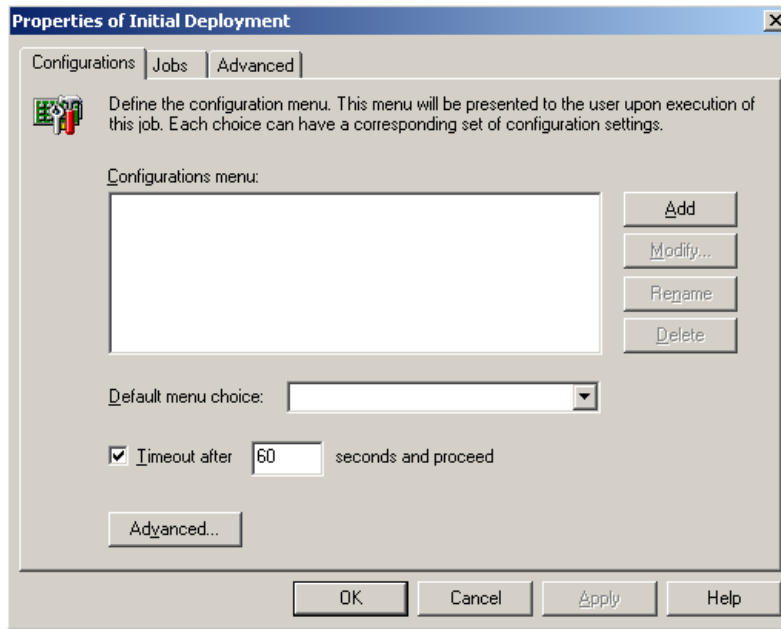


Figure 3-1 The Properties of Initial Deployment showing the Configurations tab

Clicking **Add** opens the New Job Wizard's Configuration window as shown in Figure 3-2 on page 82.

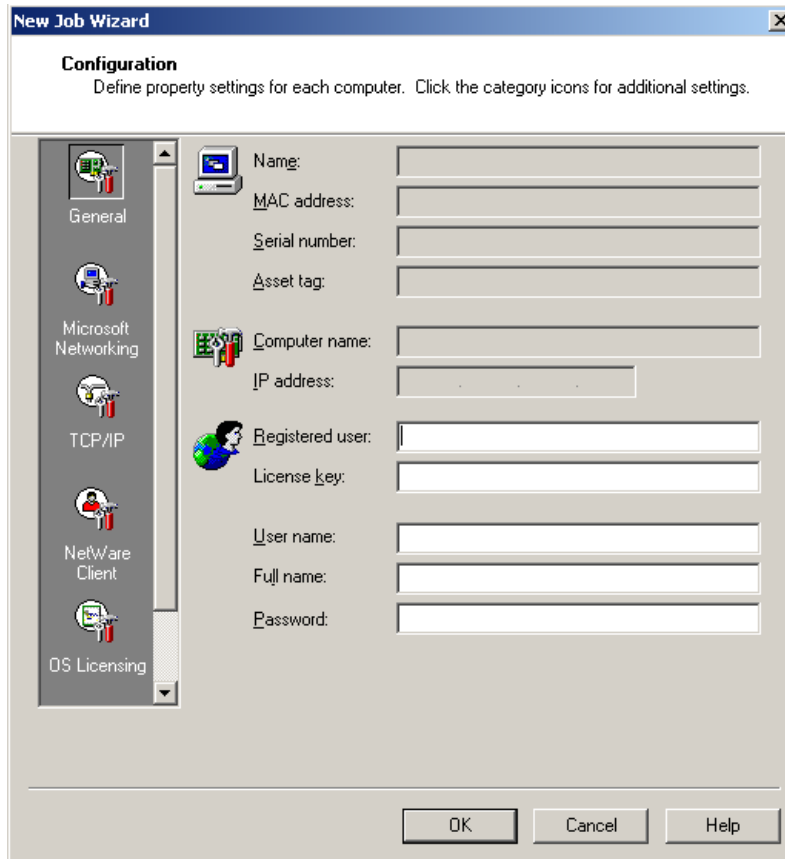


Figure 3-2 The New Job Wizard's Configuration window

The New Job Wizard's Configuration window allows you to configure a profile for your computer(s). The profile can be used for the following:

- ▶ Create User accounts and associate the accounts to specific groups
- ▶ Customize the computer NetBIOS name using tokens
- ▶ Join the computer(s) to a specific Workgroup or a Domain
- ▶ Configure multiple NICs with advanced networking

The extent to which you can customize computers with Initial Deployment will not be covered in this redbook, however you can get more information about Initial Deployment in the *Altiris Deployment Solution 6.5 Reference Guide*, available from:

<http://www.altiris.com/Support/Documentation.aspx>

When you have finished customizing your profile, click **OK** to return to the Configurations tab.

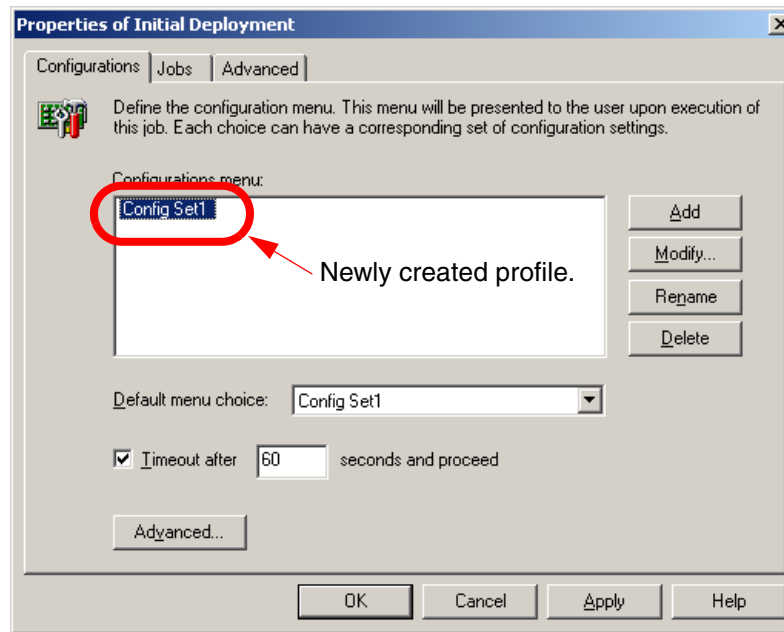


Figure 3-3 The Properties of Initial Deployment showing the Configurations tab with one profile created

When you have created a profile it will show in the list box as shown in Figure 3-3.

Clicking **Modify** opens the New Job Wizard's Configuration window, which enables you to make additional changes to the selected profile. Clicking **Rename** enables you to rename the currently selected profile. Clicking **Delete** removes the currently selected profile from the Configurations menu permanently. There is no undo feature, so be very careful when deleting profiles.

You can specify a default menu option by using the **Default menu choice** pull-down menu.

The check box below the Default menu choice text box enables you to set a time-out time in seconds for the user to respond with a profile choice before using the default menu option and proceeding with the deployment. If this is unchecked, deployment will wait indefinitely for user interaction.

Clicking **Advanced** opens the Advanced Configuration window. This window allows the user to define a time to run the job.

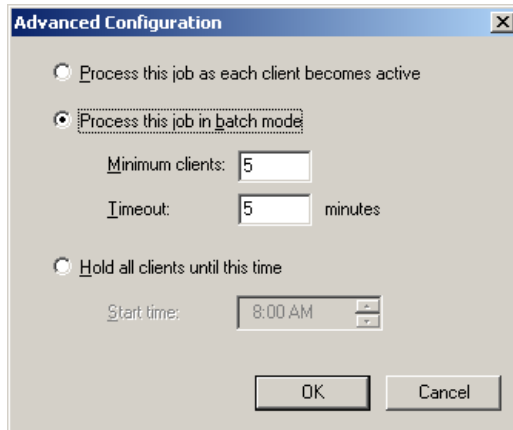


Figure 3-4 The Advanced Configuration window

There are three options available on the Advanced Configuration window:

- ▶ **Process this job as each agent becomes active:** If selected, the defined job(s) will run as soon as a computer is powered on and contacts the Deployment Server.
- ▶ **Process this job in batch mode:** If selected, this option allows you to stagger the deployment with time intervals between batches.

For example, let's say you are deploying ten new computers and want to deploy five at a time with a five minute interval between batches. You can enter the number of client computers as the minimum in a batch by entering a number for **Minimum clients** (in our example we enter 5). In the **Timeout** text box, you can enter the number of minutes to delay between the next batch. (In our example we enter 5 to wait five minutes before executing the next batch.) Using this method prevents power surges and reduces the stress on the Deployment Server.

- ▶ **Hold all clients until this time:** If selected, you can specify a set time to run the job (or jobs).

Make your selection and click **OK** to return to the Configurations tab.

Note: If you do not create any custom profiles, the deployment process will automatically set TCP/IP information to use DHCP and will set the NetBIOS name to match the computer's serial number, MAC address or asset tag.

3.1.2 Jobs tab

The **Jobs** tab allows you to add existing jobs or to create new jobs to run on the new computers. The jobs you add or create will be listed in a menu and presented to the user when the target computer(s) contact the Deployment Server.

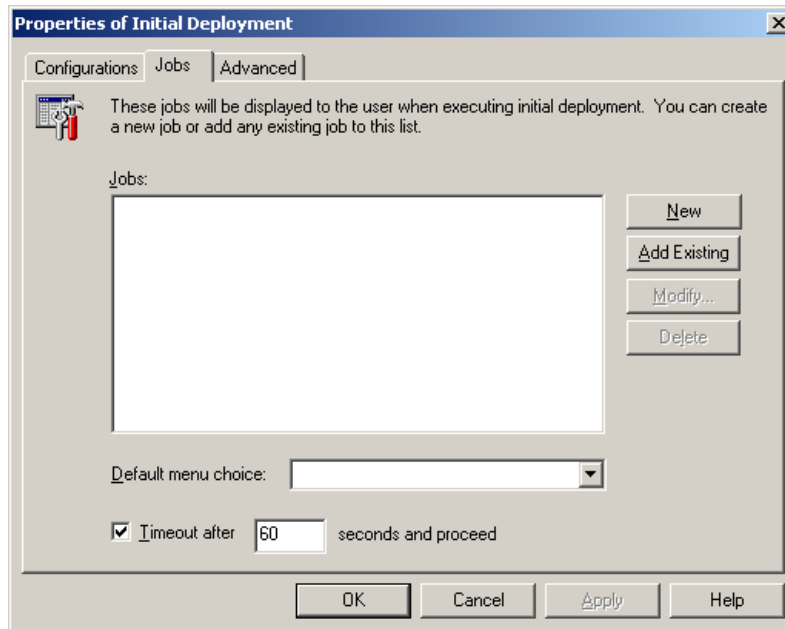


Figure 3-5 The Properties of Initial Deployment window showing the Jobs tab

Creating a new job for Initial Deployment

To create a new job to use as for Initial Deployment rather than an existing job follow the steps below:

1. Clicking **New** opens the **Select a Folder** window. This window displays the existing folders in the Jobs pane of the Deployment Console. Select a folder in which to create the new job. Click **OK** to continue.

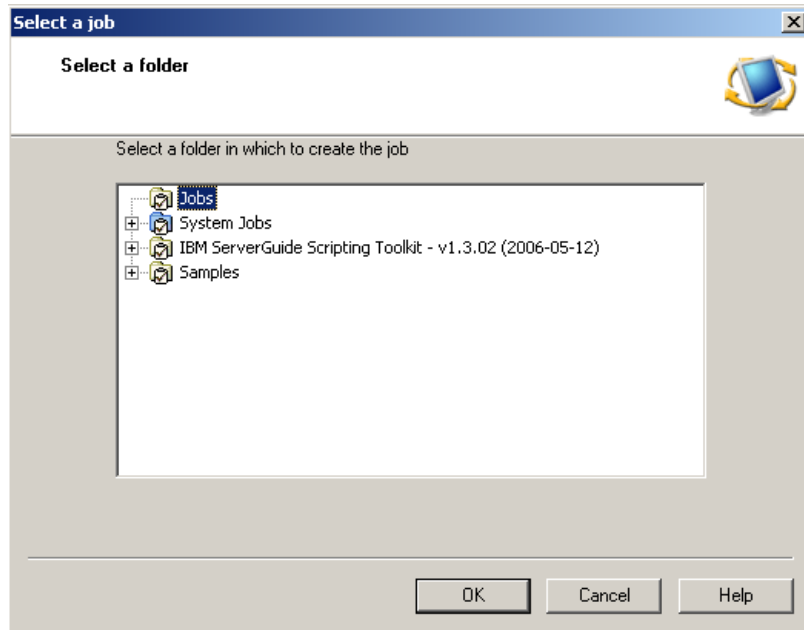


Figure 3-6 The Select a folder window

2. When the Job Properties window loads, give the job a meaningful name by entering text in the **Name** text box. If you want to write a description for the job enter the text in the text box labeled **Description**. Click **Add** to add tasks to the job.

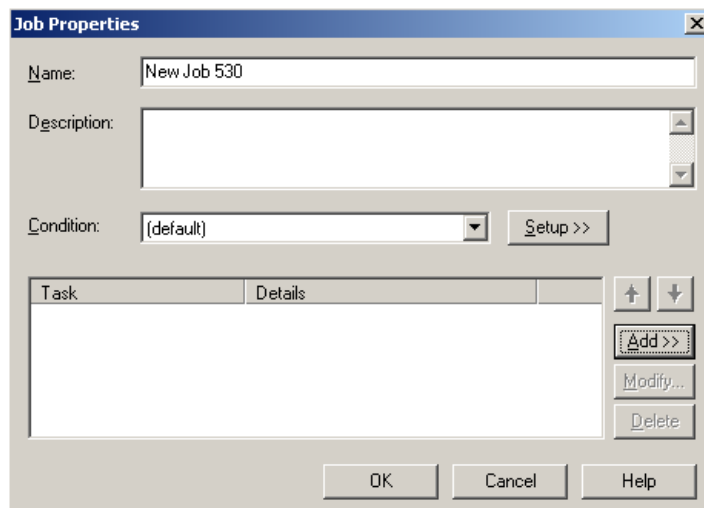


Figure 3-7 The Job Properties window

3. When you click Add, the menu in Figure 3-8 is displayed. Select the type of task you want to add and configure it accordingly. Refer to the *Altiris Deployment Solution 6.5 Reference Guide* for more information about the creation of job tasks.

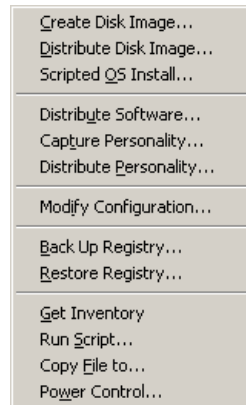


Figure 3-8 The Add Task menu

4. After you configure your task and have returned to the Job Properties window, you can click **Add** to add more tasks or you can click **Modify** to edit an existing task. If you want to delete a task, select the task and click **Delete**.
5. When you have finished configuring your job, click **OK** to return to the Properties of Initial Deployment window. From here you can add more jobs to the Initial Deployment menu or you can click **OK** to complete the configuration of the Initial Deployment.

Adding an existing job to Initial Deployment

To use a pre-existing job to Initial Deployment follow the steps below:

Click **Add Existing** on the Properties of Initial Deployment window shown in Figure 3-5 on page 85. This opens the Select a job window as shown in Figure 3-9 on page 88. The Select a job windows displays the entire contents of the Jobs pane of the Deployment Console (minus the Initial Deployment job). Select the job you want to use and click **OK** to return to the Properties of Initial Deployment window. From here you can add more jobs to the Initial Deployment menu or you can click **OK** to complete the configuration of the Initial Deployment.

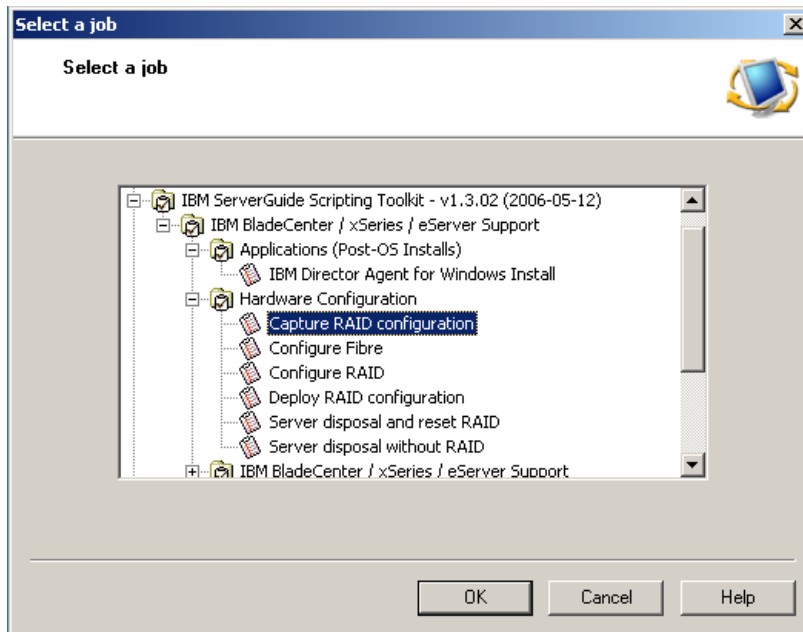


Figure 3-9 The Select a job window

3.1.3 Advanced tab

Deployment Solution has a feature that prevents an unmanaged computer of a certain class (server or workstation) from being accidentally imaged or re-imaged when running a PXE initial deployment job. By default, this safety feature is enabled by allowing Initial Deployment to be run on only server class computers.

To enable Initial Deployment for workstations, select **Workstation/Clients**.

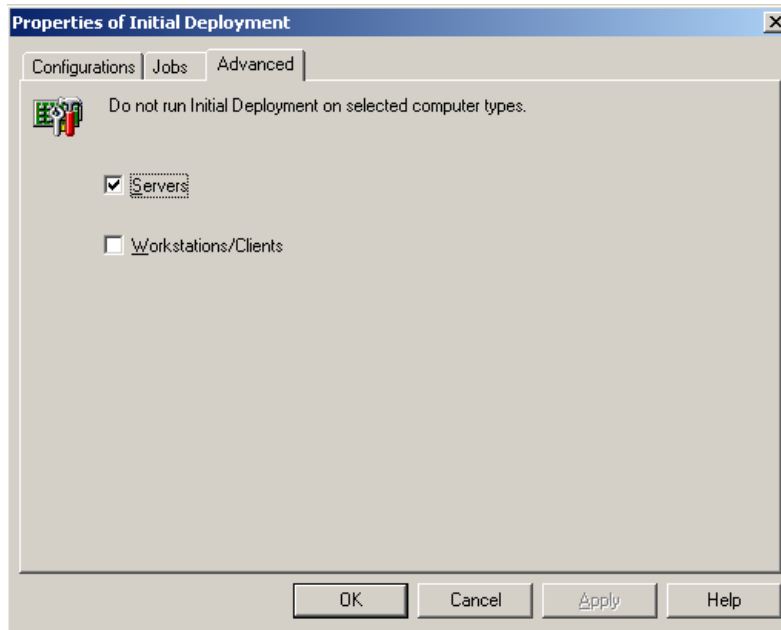


Figure 3-10 The Properties of Initial Deployment window showing the Advanced tab

3.2 Pre-staging computers for deployment

A very nice feature of Altiris Deployment Solution is the ability to pre-stage computers. Pre-staging one or more computers in the Deployment Console allows you to enter or import information such as IBM serial number, MAC address, asset tag, NetBIOS name, IP address and domain information into the Deployment Database before the computer connects to the Deployment Server for the first time.

This feature allows you to create *virtual computers* and assign jobs to them before the computers have even arrived at your site. For example, you order a new BladeCenter with fourteen HS20 Blade computers. You can ask your account representative for the serial number of every computer. Using the serial numbers of the computers, you can create virtual computers in the Deployment Console. When the virtual computers have been created you can assign jobs and configuration tasks to them.

Note: The term *virtual computer* does not refer to virtualized computers as in Microsoft Virtual Server or those created using VMware. In this context it refers to a record in the Deployment Database that is created before the computer has ever contacted the Deployment Server.

When the new computers connect to the Deployment Server they are compared against existing records in the Deployment Database. One of three IDs: serial number, MAC address, or asset tag is compared against records in the Deployment Database. Since they have been pre-staged, the computers are recognized as managed computers and any jobs that have been assigned to the pre-staged virtual computer will now execute.

There are two ways to enter pre-staging information:

- ▶ Manually, one by one, on the Deployment Console. This method is sufficient if you have only a few computers to deploy.
- ▶ By importing a CSV text file. This method is best for a large number of computers.

Each of these methods are discussed in the following sections.

3.2.1 Pre-staging computers manually from the Deployment Console

The pre-staging of computer accounts makes for flexible planning and can save time with deployment. You can stage the new computers in the Deployment Console before the computers are connected to the Deployment Server or powered up. When the new computer is connected, you will be ready to deploy because you have done all the preparation work ahead of time.

To pre-stage a computer, follow the steps below:

1. On Deployment Console, click **File** → **New** → **Computer**. The New Computers window loads.

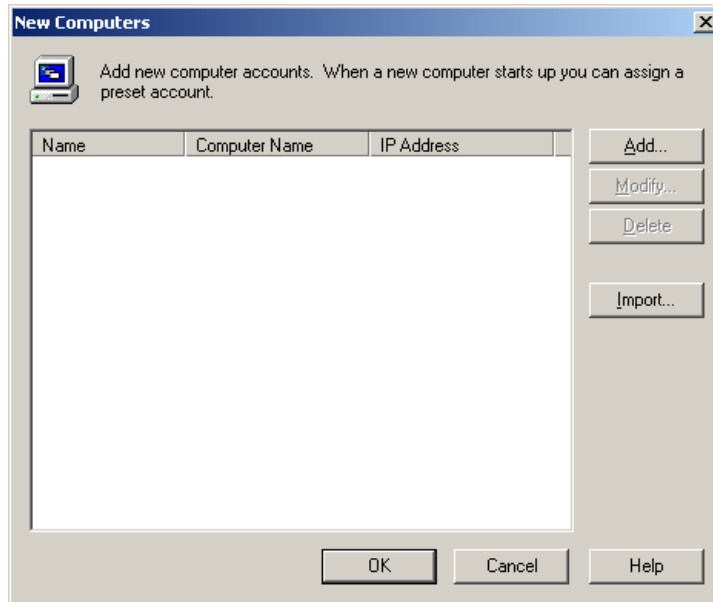


Figure 3-11 The New Computers window

2. Click **Add** to open the New Computer Properties window. Configure the computer as appropriate for your environment. Be sure to enter the correct serial number in the field labeled **Serial number**, in the General section of the New Computer Properties window. When you have finished configuring your computer, click **OK** to return to the New Computers window.

For more information about configuring computers, refer to the *Altiris Deployment Solution 6.5 Reference Guide*.

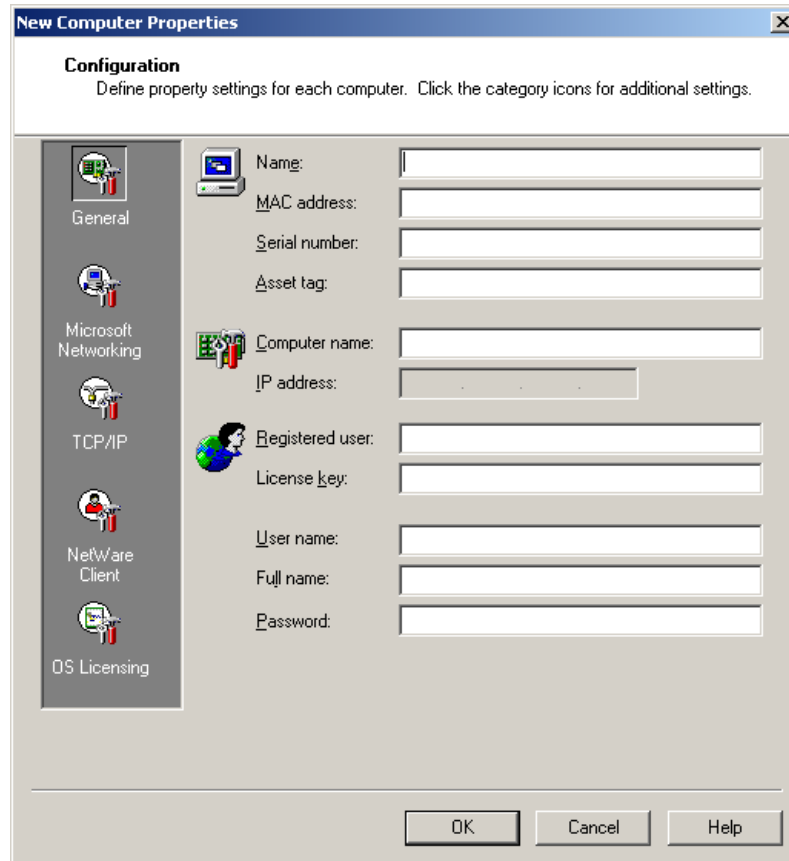


Figure 3-12 The New Computer Properties window

3. To pre-stage another computer, click **Add** to return to the New Computer Properties window and configure the next computer.
4. The virtual computers you just added will show up in Computers pane of the Deployment Console. The computer icons in the Computers pane will be yellow to differentiate the virtual computers from the managed computers.
5. Drag any jobs you want to assign to any of the computers. When the computer contacts the Deployment Server for the first time the job will execute.

3.2.2 Pre-staging computers using a CSV file

When pre-staging a large number of computers you can import several computers at one time using a CSV file. The format of the file can be either in a text format or in a spreadsheet format (.XLS)

Note: Two sample computer import files are available in the samples directory within the Deployment Share. The files are named: ImportComputer55.txt and ImportComputer55.xls

These files can be used as a templates for entering your own computers. Open and examine the syntax and column headers within the files.

To create your own CSV text file follow the steps below:

1. Browse to the samples directory in the Deployment Share.
2. Make a copy of the **ImportComputers55.txt** file and open it in Notepad.
3. Enter minimum information like Display name, Serial number, NetBIOS name, and then the flag for DHCP or static IP address information using the syntax shown in the file. Save the file using a name of your choosing.
4. On the Deployment Console, click **File** → **Import/Export** → **Import Computers** from the main menu.
5. Browse to the CSV text file you saved and click **Open**.
6. An informational message showing the number of computers being imported will appear. Click **OK** to continue.
7. The virtual computers you just imported via the CSV text file will show up in Computers pane of the Deployment Console. The computer icons in the Computers pane will be yellow to differentiate the virtual computers from the managed computers.
8. Drag any jobs you want to assign to any of the computers. When the computer contacts the Deployment Server for the first time the job will execute.

3.3 Linking multiple deployment jobs together

A job is a collection of defined deployment tasks. You can build new jobs with tasks to automatically create or deploy hard disk image, install patches and hotfixes, distribute software packages, change computer settings, and so on. These jobs can be run immediately or can be schedule to run at a later time.

The New Job Wizard can guide you through common deployment and management tasks. You build jobs by adding task to a job and customize the task to fit your needs. Refer to Chapter 7, “Building and Scheduling Jobs” of the *Altiris Deployment Solution 6.5 Reference Guide* for details.

There may be instances where you have many small jobs and you want to tie them together to build a new “super job” to run multiple common tasks. For example, after a base operating system image is deployed to a new computer, you may want to do the following small tasks:

- ▶ Configure the networking
- ▶ Join the domain
- ▶ Install required software products such as anti-virus or backup clients

Rather than dropping several jobs onto a computer to perform the various tasks, you can consolidate them all into one super job. Dropping the super job onto a computer will perform all the deployment tasks that were associated with the multiple deployment tasks before.

Follow the steps below to create a super job:

1. Open the Deployment Console.
2. Decide which deployment jobs you want to consolidate. For this example we will be consolidating the Configure RAID job with an image deployment job. This is a common two-step process when deploying new computers.
3. Select the **Configure RAID** job, located in the Jobs pane of the Deployment Console in the folder “IBM ServerGuide Scripting Toolkit - *Version_Number (Date_Released)* → IBM BladeCenter / xSeries / eServer Support → Hardware Configuration”, where *Version_Number* is the version of ServerGuide and *Date_Released* is the date it was released to the IBM Web site.

Right-click the two tasks that make up the job in the details pane of the Deployment Console. Select **Copy** from the context sensitive menu.

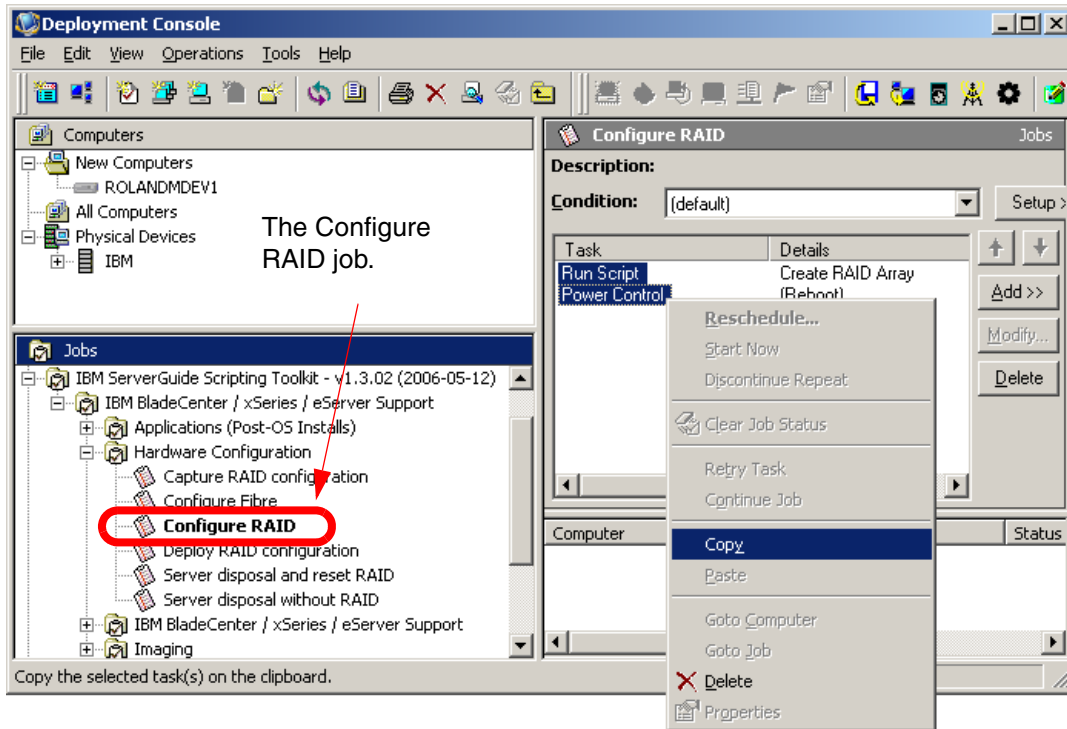


Figure 3-13 The Deployment Console with the Configure RAID job shown

4. Now select an image deployment job and make a copy for you to edit. For this example we will use the Deploy Windows Image job located in the folder "IBM ServerGuide Scripting Toolkit - *Version_Number (Date_Released)* → IBM BladeCenter / xSeries / eServer Support → Imaging.
5. Select the new copy of the imaging job and right-click in the details pane of the Deployment Console. Select **Paste** from the context sensitive menu to paste the Configure RAID tasks into the new image deployment job.
6. Re-order the job tasks, by using the up and down arrows in the details pane, so the tasks that make up the Configure RAID job run sequentially before the tasks that make up the image deployment job.

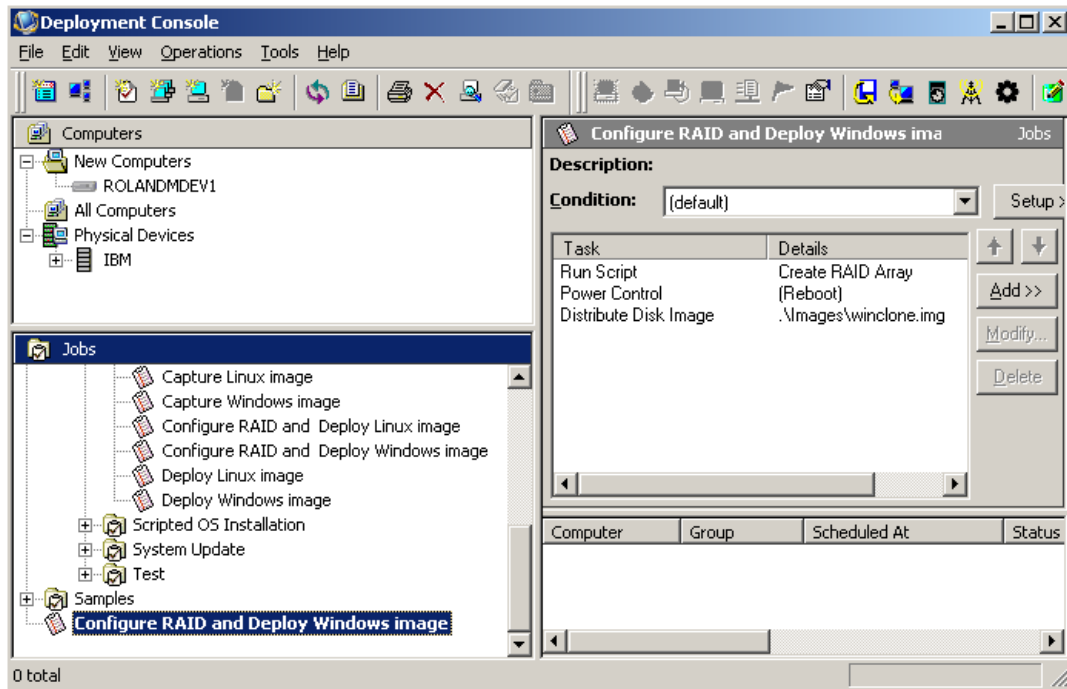


Figure 3-14 The custom super job to configure RAID and then deploy a Windows image

Drop the newly created super job onto an active computer or group of computers to configure the RAID and to deploy a Windows image.

3.4 Job troubleshooting

When creating custom jobs it is likely that on occasion a task will fail causing the entire job to fail. There are many reasons why a task could fail. Most likely there is a problem with syntax in one of the scripts, or perhaps a file cannot be located.

In this section we will look at how to determine when a job has failed, and then how to identify the failing task.

Note: In Chapter 29, “Error Messages in Deployment Solution” of the *Altiris Deployment Solution 6.5 Reference Guide*, Altiris provides information about error messages created by RapiDeploy with explanations, possible cause and recommended actions.

How to determine a job has failed

In most cases determining a job has failed is very easy. An icon with a red X (rather than a green check mark) will be displayed in the details pane of the Deployment Console as shown in Figure 3-15.

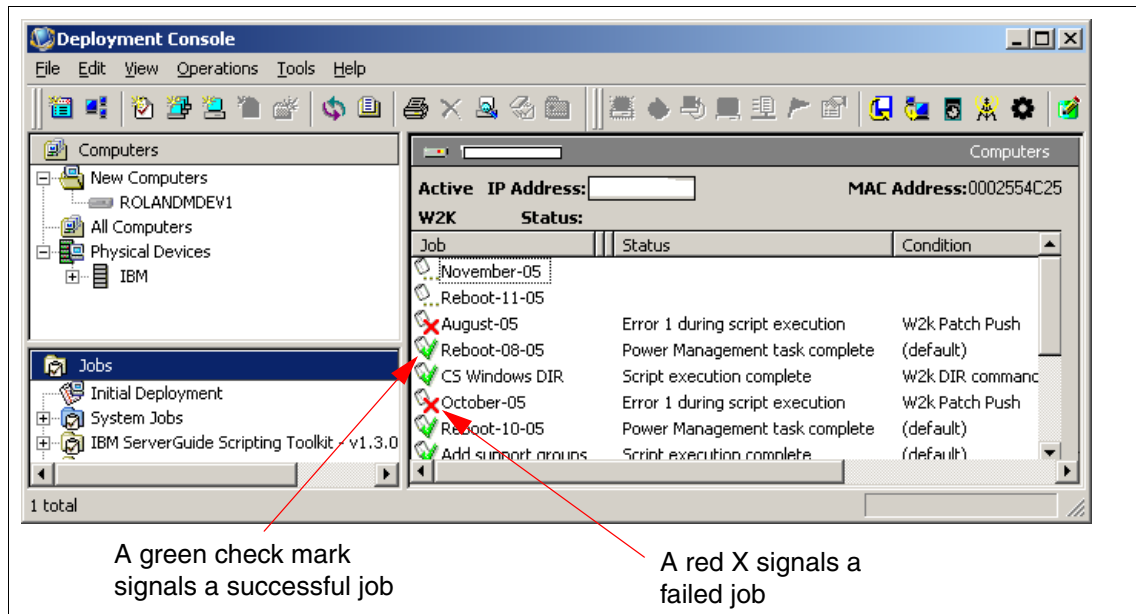


Figure 3-15 The Deployment Console showing failed jobs

Occasionally a job can fail without the Deployment Server knowing it. If the Deployment Server is unable to gain control of the target computer upon a reboot (perhaps the target computer does not have PXE configured correctly and missed the PXE offering) the status of the job will be Sending Wake-On-Lan signal. This generally means the Deployment Server is unable to connect to target computer to execute the task.

On some occasions a job will show as being successful (by displaying a green check mark), but from the point of the user the job failed. This is very common in image deployment. The Deployment Server considers the job a success if the image has been successfully transferred to the target computer. However, from the user's point of view the job is not successful until you have a working operating system on the target computer.

If the proper SCSI device drivers were not included with the operating system image, the image will not boot successfully, but from the Deployment Server's point of view the job was a complete success. Another common example is the Configure RAID job. The Deployment Server considers this job a success as

soon as the script is delivered to the target computer and executed. However, that does not mean the ServeRAID™ adapter was successfully configured. We recommend verifying the jobs are successful according to the job's purpose.

Troubleshooting the failed job

To get more detail about a failed job, or to check the status of a running job, simply double-click the job icon in the details pane of the Deployment Console.

Double-clicking on the job icon opens the Job Schedule Information window shown in Figure 3-16. In the **Task Process** window, the various tasks that make up the deployment job are displayed along with icons that represent their current status. A green check mark means the task has completed successfully, and a red X means the task has failed. The *Altiris Deployment Solution 6.5 Reference Guide* has more information about task status and the various icons that represent the status.

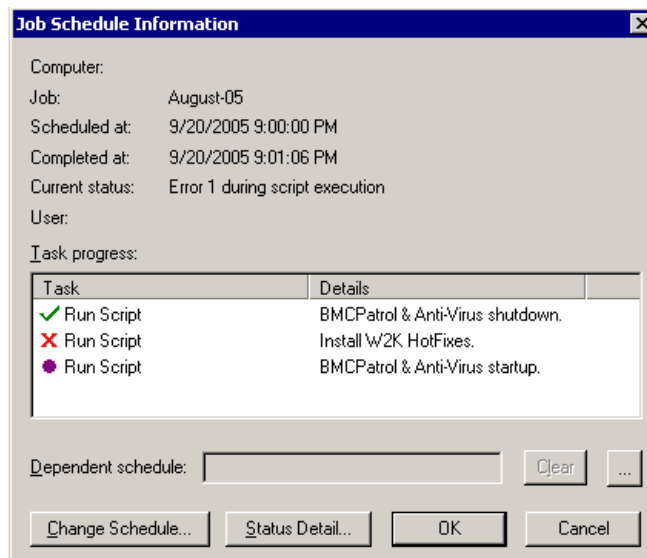


Figure 3-16 The Job Schedule Information showing deployment job tasks information

For more information, you can click **Status Detail** to open the Schedule Status Detail window (Figure 3-17 on page 99).

The Status Detail window generally displays enough information to determine the problem. At the very least it will show the task that is failing. To fix the problem, select the job and open the failing task to verify the syntax and the paths to required files.

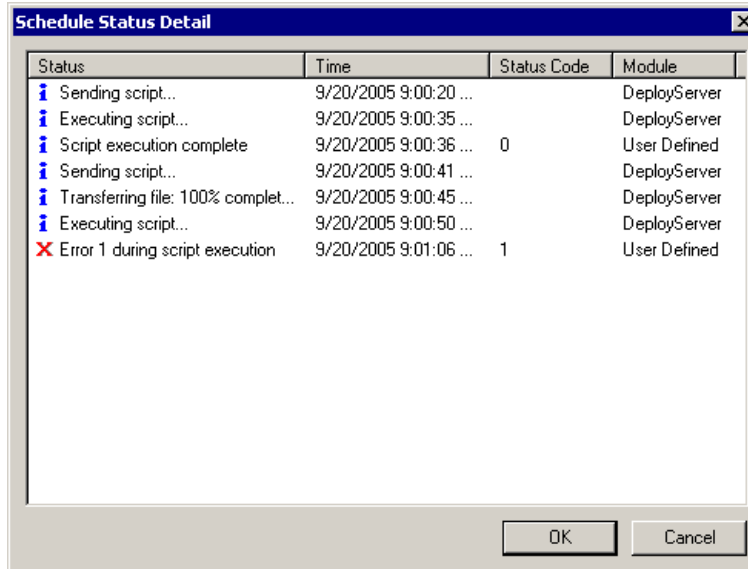


Figure 3-17 The Schedule Status Detail window

3.5 Common issues

This section lists some issues that may occur while configuring Deployment Solution. Understanding these issues and possible resolutions may help prevent them and reduce your troubleshooting time.

- ▶ Scripted operating system tasks require the drive letter F: mapped to the Deployment Share

The Scripted operating system deployment task must use mapped drive F:. The task will fail if the Deployment Share is mapped to a drive letter other than F:. This issue will not impact production network share mappings after the operating system installation because this requirement is used for this task only.

- ▶ Solaris™ agent does not support multicast server discovery

During the configuration of a Solaris system, you must provide the IP address of your Development Server.

- ▶ Windows Error 1326

You may see a “Windows Error 1326” in the Deployment Agent log if you use a UNC path and you run directly from the file source with a client that has already been authenticated to that source. This error occurs because Windows keeps tracks all network shares and users via authentications.

When you run the second time, Windows will attempt to authenticate again, but since you are authenticated from the previous use, AClient logs as Windows error 1326. This is harmless error in the AClient log. You can reboot the server to clear the authentication connection; or change users for authentication from previous job.

- ▶ Windows PE 2005 requires Windows Server 2003 SP1 for Windows PE automation

Windows PE 2005 is designed to support Windows Server 2003 Service Pack 1. It is also the first version to support Altiris Deployment Solution 6.5.

- ▶ Adding mass storage device drivers for Win PE to Boot Disk Creator Configuration

A DOS or Win PE boot disk by default does not recognize the ServeRAID-8i RAID controller with SAS drives. The ServeRAID-8i controller and SAS drives are commonly configured in X3 Architecture servers such as the x3800, x260, x3850, x366, x3950, and x460 servers. Also Boot Disk Creator does not provide an interface to allow users to install drivers for any mass storage devices that are not supported directly by Windows PE 2005.

These device drivers must be added manually to the proper directory in the Windows PE configuration in Boot Disk Creator. Refer to *Altiris Deployment Solution 6.5 Reference Guide* for detailed instructions.

- ▶ Network error during Win PE boot

If you get a network connection error during Win PE boot, you should increase the default time-out period to 180 in startup.bat file in the Boot Disk Creator configuration.

- ▶ Intel® VM adaptor needs correct DOS NIC driver

If you have an Intel VM adapter in your System x computer, to make a boot disk, you want to use the “NIC Driver for Intel Pro100ve-Dell 170L” device driver rather than the “Intel PRO 100 and 100 VM adaptor Family” device driver.

- ▶ Unable to import boot configurations from prior versions of the Boot Disk Creator

You must re-create any boot disk configurations from prior versions of the Boot Disk Creator when migrating to Altiris Deployment Solution 6.5. Older boot configurations are incompatible with the latest version of Deployment Solution because of the addition of boot media types and changes to the PXE environment.

- ▶ Error 16 while loading Windows PE PXE image

You may see an “error 16” when there is not enough RAM available on the target computer to load the ramdisk image for Windows PE. You must have at

least 256 MB RAM available on the target computer to load the image. 386 MB RAM or more is recommended.

- ▶ Win PE hangs during boot

If a computer hangs and becomes unresponsive when booting into Win PE, it most likely is caused by an incorrect or outdated NIC driver. You should obtain the latest version of the NIC device driver from the IBM Web site.

- ▶ Linux automation does not support AMD K6 or K6-2

The Linux automation environment does not support AMD K6 or K6-2 processors. If your systems have these processors, you will need to use DOS or Win PE as your automation environment.

- ▶ PXE menu supports up to 23 entries

Do not create more than 23 boot options on the PXE menu. If more than 23 PXE menu options are provided, the wrong menu selection will be returned to the Deployment Server.

- ▶ PXE menu allows same names for multiple entries

The PXE Configuration utility does not check for duplicate names when creating new PXE boot menu options. Take care not to enter duplicate names as there will be no way to distinguish one from another.

- ▶ DOS does not support fully-qualified host names

When using DOS as your automation environment, you must use the IP address for the host, not fully-qualified host name.

- ▶ Do not modify PXE configurations when jobs are in progress

When PXEConfig modifies a PXE configuration parameter or boot image, all PXE servers are updated with the new configuration and then restarted. If a PXE server is downloading a boot image to target computers, this restart will interrupt the download and could leave the target computers in an unmanageable status requiring them to be manually rebooted. You should coordinate a schedule with other support personnel for the PXE configuration change to make sure no one will download images during your PXE configuration change.

- ▶ Adding mass storage device drivers for Linux automation to Boot Disk Creator configurations

On the Linux NIC wizard page in Boot Disk Creator, click **Have Disk** to add mass storage device drivers. Mass storage device drivers can be added in a similar way to the way network device drivers are added.



IBM hardware configuration and updating

Altiris Deployment Solution integrates with the IBM ServerGuide Scripting Toolkit to offer greater manageability and flexibility when working with IBM BladeCenter and System x servers. In this chapter, we explore some of the advanced functions facilitated by the Scripting Toolkit with a focus on hardware configuration and system updating.

In this chapter we cover the following subjects:

- ▶ 4.1, “System updates” on page 104
- ▶ 4.2, “Hardware configuration” on page 120

4.1 System updates

Keeping computers up to date with BIOS updates and device drivers is a daunting task for any IT administrator. Through its alliance with Altiris, IBM is making a commitment to reducing the time and effort of keeping an up-to-date IT environment.

4.1.1 Updating system BIOS

The IBM ServerGuide Scripting Toolkit provides Altiris Deployment Solution with a job to update system BIOS on IBM BladeCenter or System x servers. The job, which is installed with the ServerGuide Scripting Toolkit, is labelled **Perform BIOS update** and can be found in the Jobs pane of the Deployment Console under **IBM BladeCenter / xSeries / eServer Support** → **System Update**.

Note: The folder labelled **IBM BladeCenter / xSeries / eServer Support** can be found inside the folder below, which is located in the Jobs pane of the Deployment Console:

IBM ServerGuide Scripting Toolkit - *version_number* (*release_date*)

Where *version_number* is the version of the ServerGuide Scripting Toolkit on which the jobs in the folder labeled **IBM BladeCenter / xSeries / eServer Support** are based and *release_date* is the date this version was released.

When a new version of the ServerGuide Scripting Toolkit is released and installed, new jobs are added to the Deployment Console. The jobs are added in a new folder to negate the possibility of overwriting any customized jobs from previous versions of the ServerGuide Scripting Toolkit.

The job does not need any task customization before being deployed, however, the BIOS flash files must be copied to the Deployment Share before you can update any computers.

Follow the steps below to prepare for BIOS updating:

1. In Windows Explorer, open the Updates folder, which is located in the ServerGuide Scripting Toolkit source tree (sgdeploy) in the deployment share.
2. Create a new folder using the machine type of the system which you want to update.

In this example we will update the BIOS of a x345 which has the machine type 8670. Create a new folder and name it "8670".

Note: The folder name must match the machine type of the computer to which you are planning on deploying the BIOS update. When deploying a BIOS update job, Altiris Deployment Solution will query the target computer for its machine type. It then looks for the directory with a name matching the machine type of the target computer.

Note also that the BIOS code must be DOS-based. This scenario does not support the Windows-based **wflash** or Linux-based **lflash** utilities.

3. Open the newly created 8670 folder and within it create a new folder named BIOS.
4. Now that the directory structure has been created, we need the actual BIOS flash files. Go to the IBM Support Web site and download the latest BIOS firmware for your Target System (in our example the x345). The IBM Support Web site can be found at the following URL:
<http://www.ibm.com/support>
5. When the diskette image has downloaded, extract the image to a diskette and then copy the contents of the diskette to the BIOS folder within the 8670 directory.

The **Perform BIOS update** job is ready to deploy to your target computers when you have completed the steps above. However, if you want to modify the **Run BIOS Update** task in the **Perform BIOS update** job, the following table describes the customizable variables.

Table 4-1 Definitions for the variables in the Run BIOS Update task

Variable Name	Description	Default
UPD_BDIR	The base directory that contains the BIOS code and update files in the source tree.	%MACHTYPE%\bios
UPD_BIOS	Specifies whether to perform BIOS code updates. Valid values are Y or N.	Y
UPD_PATH	The fully qualified path to the BIOS code and firmware code update files in the source tree.	%TAS_PATH%\updates (f:\sgdeploy\updates)

To update the system BIOS on a computer, drag-and-drop the job labelled **Perform BIOS Update** onto an active computer or group of computers in the Computers pane of the Deployment Console.

4.1.2 Capturing and deploying CMOS settings

The IBM ServerGuide Scripting Toolkit provides Altiris Deployment Solution with jobs to capture and deploy CMOS settings on IBM BladeCenter or System x Servers. The jobs, which are installed with the ServerGuide Scripting Toolkit, are labelled **Capture CMOS settings to a binary file** and **Deploy CMOS settings from a binary file** and can be found in the Jobs pane of the Deployment Console in path **IBM BladeCenter / xSeries / eServer Support → System Update**.

Note: Target computers must be the same machine type as the Reference Computer for the CMOS update to be successful.

Capturing CMOS Settings

The capturing of CMOS (BIOS) settings is functionally very similar to updating the system BIOS. Before capturing the CMOS settings you must follow the steps outlined in 4.1.1, “Updating system BIOS” on page 104. The necessary BIOS files must be set up prior to using the scenario as described in 4.1.1, “Updating system BIOS” on page 104.

Tip: Capturing and deploying CMOS settings can be quite useful as a way of quickly doing routine BIOS changes such as changing the boot order of multiple computers.

The **Capture CMOS settings to a binary file** job is ready to deploy to your target computers after you have created the directory structure and populated the BIOS folder with the BIOS flash files. However, if you want to modify the **Capture CMOS settings to a binary file** task in the **Capture CMOS settings to a binary file** job, the following table describes the customizable variables.

Table 4-2 Definitions for the variables in the Capture CMOS Settings to a binary file task

Variable Name	Description	Default
CMOS_FILE	The name of the CMOS settings binary file.	cmosinfo.bin Note: File names must be in DOS-compatible 8.3 notation.
CMOS_PATH	The fully qualified path to the CMOS binary file in the source tree.	%TK_PATH%\altiris\temp\%MACHTYPE%
UPD_BDIR	The base directory that contains the BIOS code and update files in the source tree.	%MACHTYPE%\bios

Variable Name	Description	Default
UPD_PATH	The fully qualified path to the BIOS code and firmware code update files in the source tree.	%TAS_PATH%\updates (f:\sgdeploy\updates)

To capture the CMOS settings, drag-and-drop the job labelled **Capture CMOS Settings to a binary file** onto an active computer or group of computers in the Computers pane of the Deployment Console.

When scheduled to run on the Reference Computer, the job creates a binary file documenting the current CMOS settings of the Reference Computer. The file is saved as `cmosinfo.bin` in the ServerGuide Scripting Toolkit source tree in folder `.\sgdeploy\altiris\temp\MachineType\`, where *MachineType* is the machine type of the Reference Computer.

Deploying CMOS Settings

After you have captured the CMOS settings of the Reference Computer you can deploy those settings to multiple target computers of the same model type as the Reference Computer. Drag-and-drop the job labelled **Deploy CMOS settings from a binary file** onto an active computer or group of computers in the Computers pane of the Deployment Console.

When the job runs it looks in the aforementioned directory, with *MachineType* being the machine type of the target computer, for the file named `cmosinfo.bin`. If the file is located, the **Deploy CMOS settings from a binary file** job updates the Target System's CMOS with the settings saved in the binary file.

4.1.3 Updating ServeRAID BIOS/firmware

The most recent release of the ServerGuide Scripting Toolkit included support for updating the BIOS/firmware of the 4H, 4Mx, 4Lx, 5i, 6i, 6i+, 6M, 7k, and 8i ServeRAID controllers. The job is labelled **Perform IBM ServeRAID BIOS/firmware update** and can be found in the Jobs pane of the Deployment Console in folder **IBM BladeCenter / xSeries / eServer Support → System Update**.

Follow the steps below to prepare for updating the BIOS/firmware for a supported ServeRAID controller:

1. Before updating the ServeRAID BIOS/firmware of a supported controller, a folder must be created within the updates folder (located in the `sgdeploy` directory in the Deployment Share). The folder name varies depending on the ServeRAID controller you want to update. If you are updating the 4H, 4Mx,

4Lx, 5i, 6i, 6i+, 6M, or 7k ServeRAID controllers, create a folder named SRVRAID. If you are updating the 8i, create a folder named SVRAID8I. The final path should look like the following for the 4H, 4Mx, 4Lx, 5i, 6i, 6i+, 6M, or 7k ServeRAID controllers:

.\sgdeploy\updates\SRVRAID

or if you are updating the BIOS/firmware of the 8i ServeRAID controller:

.\sgdeploy\updates\SVRAID8I

2. Now that the directory structure has been created, we need the actual BIOS/firmware flash files. Go to the IBM Support Web site and download the latest BIOS/firmware for your supported ServeRAID controller. The IBM Support Web site can be found at the following URL:

<http://www.ibm.com/support>

3. When the diskette image has downloaded, extract the image to a diskette and copy the contents of the diskette to the correct folder within the updates folder.

The **Perform IBM ServeRAID BIOS/firmware update** job is ready to deploy to your target computers when you have completed the steps above. However, if you want to modify the **Run IBM ServeRAID BIOS/firmware update** task in the **Perform IBM ServeRAID BIOS/firmware update** job, the following table describes the customizable variables.

Table 4-3 Definitions for the variables in the Run IBM ServeRAID BIOS/firmware update task

Variable Name	Description	Default
UPD_SR	Whether you want to update the ServeRAID controller BIOS	Y
UPD_PATH	The fully qualified path to the updates folder in the sgdeploy directory.	%TAS_PATH%\updates
UPD_SDIR	The fully qualified path to the BIOS/firmware update file in the sgdeploy directory for the 4H, 4Mx, 4Lx, 5i, 6i, 6i+, 6M, and 7k ServeRAID controllers.	SRVRAID
UPD_SV8I	The fully qualified path to the BIOS/firmware update file in the sgdeploy directory for the 8i ServeRAID controller.	SVRAID8I

To update the BIOS/firmware of a supported ServeRAID controller installed in a computer, drag-and-drop the job labelled **Perform IBM ServeRAID BIOS/firmware update** onto an active computer or group of computers in the Computers pane of the Deployment Console.

4.1.4 Additional updates

With the integration of the ServerGuide Scripting Toolkit, updates to components such as diagnostics, BMC firmware, network adapter firmware, host bus adapter firmware, and any other type of update that requires the computer to boot to a diskette can be performed on System x systems. Although no specific jobs have been provided for these types of updates, the tools and batch files necessary to perform the updates are installed with the ServerGuide Scripting Toolkit. No changes to the ServerGuide Scripting Toolkit tools are required to perform the additional updates.

In this section, we cover populating the ServerGuide Scripting Toolkit source tree with the diagnostic update files, the creation of an unattended diagnostics firmware update job, and the creation of a batch file that will launch the update.

Note: This method will not work for all firmware updates. Some System x computers use chipsets that require updates that do not support unattended firmware updating. After downloading and extracting the firmware update for your System x computer, open the readme file and verify that unattended firmware updating is supported.

Note also that some firmware updates are not fully automated. It is possible to launch the update, but the update might require user intervention to complete.

To populate the ServerGuide Scripting Toolkit source tree, follow the steps below:

1. In Windows Explorer, open the Updates folder, which is located in the ServerGuide Scripting Toolkit source tree (sgdeploy) in the Deployment Share.
2. Create a new folder using the machine type of the system that you want to update as the name.

In this example we update the diagnostics of an x336 that has the machine type 8837. Therefore new folder should be named 8837.

Note: The folder name must match the machine type of the computer to which you are planning to deploy the diagnostics update. When deploying a diagnostics update job, Altiris Deployment Solution will query the target computer for its machine type. It then looks in the Updates folder for a folder with a name matching the machine type of the target computer.

Note also that the diagnostic code must be DOS-based. This scenario does not support the Windows-based `wflash` or Linux-based `lflash` utilities.

3. Open the newly created 8837 folder and within it create a new folder named DIAG.
4. Now that the directory structure has been created, we need the actual diagnostic flash files. Go to the IBM Support Web site and download the latest diagnostic firmware for your target computer (in our example the x336). The driver and download matrix for System x servers is at:
<http://www.ibm.com/pc/support/site.wss/MIGR-4JTS2T.html>
5. When the diskette images have been downloaded, extract the images to diskettes and then copy the contents of the diskettes to the DIAG folder within the 8837 directory.
6. Open the readme.txt file from either of the diskettes. Scroll down to the section labeled Unattended Mode (shown below).

```
5.0  Unattended Mode
      -----

5.1  Steps for unattended mode

- Boot to DOS

- Copy flash2.exe from the "IBM xSeries 336 POST/BIOS Flash Disk"
and all *.us* files from the "IBM xSeries 336 Diagnostics Flash
Update Diskette" to the same directory on some media capable of
storing 2.5MB of data

- From the directory just copied to, run "flash2.exe /u /d"
```

Figure 4-1 The Unattended Mode section of the readme.txt file

Notice that the instructions say that the flash2.exe application is required to run the diagnostic flash update. The flash2.exe application is available on the BIOS update diskette.

7. Repeat steps 4 and 5 but instead of downloading the diagnostic flash files, download the DOS version of the BIOS flash diskette image. Copy only the flash2.exe application from the BIOS diskette to the DIAG folder in the ServerGuide Scripting Toolkit source tree.

After copying the files, the DIAG folder should resemble Figure 4-2 on page 111.

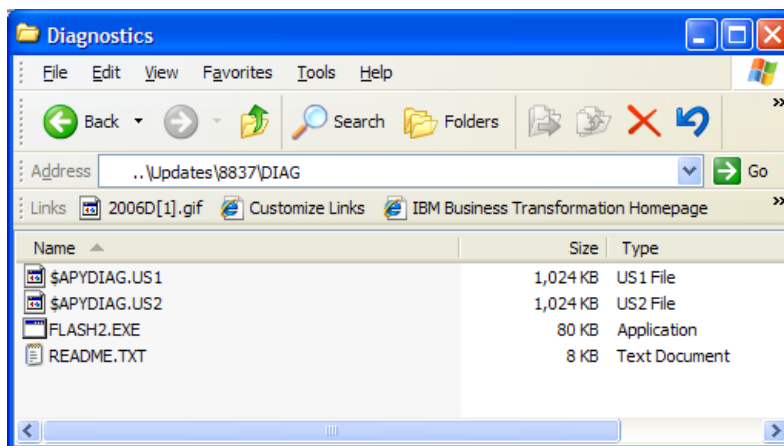


Figure 4-2 The DIAG folder after copying over all required files

After you have populated the ServerGuide Scripting Toolkit source tree, a custom deployment job must be created in the Deployment Console.

Follow these steps to build a custom deployment job:

1. Open the Deployment Console.
2. Make a copy of the job labeled **Perform BIOS update**, which is located in the Jobs pane of the Deployment Console. Rename the copy of the BIOS update job to Perform DIAG update.
3. Click the **Perform DIAG update** job you just created, and in the Details pane of the Deployment Console select the **Run BIOS update** task. Click **Modify**.
4. Scroll down the script and locate the following line:

```
set UPD_BDIR=%MACHTYPE%\BIOS
```

This variable points to the BIOS update directory that holds the BIOS firmware update files. Change *BIOS* to *DIAG* so the job will look in the DIAG folder rather than the BIOS folder for the firmware update files. The modified line should resemble this:

```
set UPD_BDIR=%MACHTYPE%\DIAG
```

5. Scroll to the bottom of the script and locate the following line:

```
call fwupdate.bat
```

This line calls a batch file that is provided by the ServerGuide Scripting Toolkit. The fwupdate.bat file contains the logic behind the RAID firmware and the BIOS firmware updating. The fwupdate.bat file will be discussed in more detail shortly.

6. Click **Next**, then click **Finish** to complete the creation of the new diagnostics update deployment job.

Before we can deploy a diagnostic firmware update, we need to “trick” the fwupdate.bat file into thinking we are performing a BIOS firmware update. To do this, we create a batch file named lcreflash.bat.

To create the lcreflash.bat file, follow these steps:

1. Open for editing the fwupdate.bat file, which is located in the ..\sgtk\examples directory path of the ServerGuide Scripting Toolkit source tree (sgdeploy).
2. Scroll down the batch file script and locate the :BIOSUPD section. Locate the following line in the BIOSUPD section:

```
if exist %UPD_PATH%\%UPD_BDIR%\lcreflash.bat goto FLSHBAT
```

This line looks in the folder you designated in the deployment job (in this case it is the *\machine_type\DIAG* folder) for the lcreflash.bat file. If the file exists, control passes to the :FLSHBAT section of the batch file, which proceeds to flash the BIOS of the computer. If the lcreflash.bat file is not found, the BIOS is not updated.

The lcreflash.bat file is key to performing additional updates without having to modify the fwupdate.bat file.

3. Open the readme.txt file located in the DIAG folder and scroll down to the section labeled Unattended Mode (shown in Figure 4-1 on page 110). The last line in the Unattended Mode section reads:

```
From the directory just copied to, run "flash2.exe /u /d"
```

The command in quotation marks is the command to run the diagnostic flash in unattended mode.

4. Open Notepad and type the following line of text as the first line of the text file:

```
flash2.exe /u /d
```

Save the file as a batch file named lcreflash.bat in the DIAG folder you created earlier. The folder should now resemble Figure 4-3 on page 113.

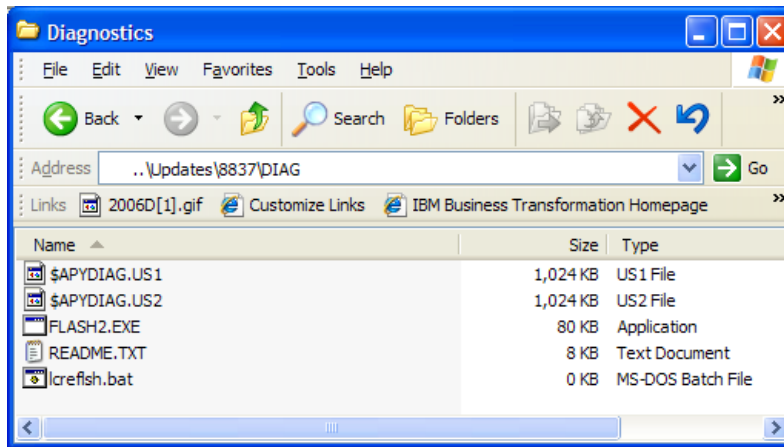


Figure 4-3 The DIAG folder after creating the lcreflash.bat file

This is all of the customization that is required to perform additional updates. Drop the newly created Perform DIAG update job onto any active x336 computers in the Computers pane of the Deployment Console to update their diagnostics firmware.

Again, this methodology can be used to perform any type of DOS-based update that can be initiated from a batch file.

4.1.5 Integrating with IBM UpdateXpress

Keeping firmware up to date no longer requires your undivided attention. By integrating Altiris Deployment Solution with UpdateXpress, a manual time-consuming process can be transformed into a task that is fast and easy.

The IBM UpdateXpress RemoteUX utility (remoteux.exe) works in any supported server environment and with a mix of operating systems. UpdateXpress enables you to maintain your systems Windows Device Driver and firmware at the most current levels, helping you avoid unnecessary outages. UpdateXpress automatically detects current device driver and firmware levels, providing the option of selecting specific upgrades or allowing UpdateXpress to update all of the system levels it detect as needing an upgrade.

UpdateXpress keeps your system running optimally by:

- ▶ Detecting the current level of system and subsystem firmware and then enabling the upgrade of firmware: BIOS, diagnostics, systems management processors, ServeRAID, tape drives, and hard disk drives

- ▶ Detecting the current level of device drivers and enabling the upgrade of Windows Device Drivers: SCSI controllers, Ethernet controllers, systems management processors, and ServerRAID controllers

The IBM ServerGuide Scripting Toolkit provides Altiris Deployment Solution with jobs to leverage integration with UpdateXpress's RemoteUX utility. The jobs, which are included with the ServerGuide Scripting Toolkit, are named:

- ▶ Run RemoteUX Driver Updates - UpdateXpress CD 1
- ▶ Run RemoteUX Firmware Updates - UpdateXpress CD 1
- ▶ Run RemoteUX Driver Updates - UpdateXpress CD 3
- ▶ Run RemoteUX Firmware Updates - UpdateXpress CD 3

These can be found in the following paths in the Jobs pane of the Deployment Console:

IBM BladeCenter / xSeries / eServer Support System Update → Windows Post-OS Updates → IBM UpdateXpress CD 1 supported servers

And for the UpdateXpress CD3 jobs:

IBM BladeCenter / xSeries / eServer Support → System Update/Windows Post-OS Updates → IBM UpdateXpress CD 3 supported servers

Before taking advantage of the integration with UpdateXpress, the media must be imported into the sgdeploy directory.

Importing UpdateXpress files into Altiris Deployment Solution

To integrate UpdateXpress with Altiris Deployment Solution you must first download the UpdateXpress CDs ISO images from the IBM Web site. The Web site can be found at the URL below:

http://www.ibm.com/servers/eserver/xseries/systems_management/ibm_director/extensions/xpress.html

UpdateXpress is comprised of three CD-ROMs:

- ▶ CD 1 contains updates for Windows-based xSeries servers.
- ▶ CD 2 is for Linux-based xSeries servers. Linux is currently not supported by the ServerGuide Scripting Toolkit integration with Altiris Deployment Solution.
- ▶ CD 3 contains updates for Blade servers.

Integrating UpdateXpress with Altiris Deployment Solution is as follows:

1. Download the ISO images for CDs 1 and 3 from the above URL.

2. Create two folders called UXCD1 and UXCD3 in the updates folder in the ServerGuide Scripting Toolkit source tree (the sgdeploy folder) within the Deployment Share, “.\sgdeploy\updates”.

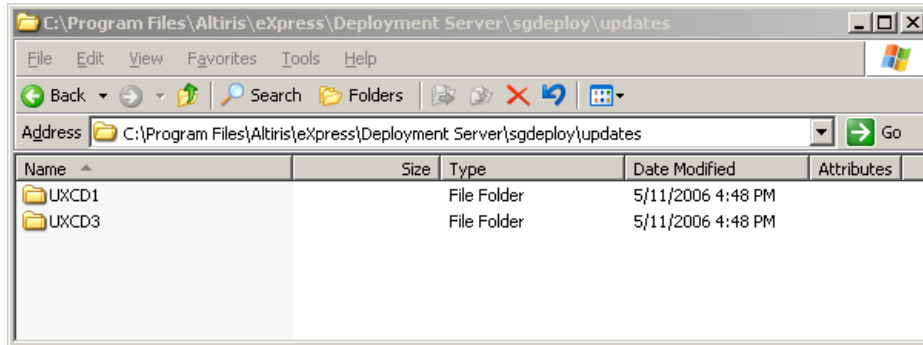


Figure 4-4 The UXCD folders created for holding the UpdateXpress CDs' contents

3. Copy the entire contents of CD1 of the UpdateXpress CD set to the UXCD1 folder you just created, next copy the entire contents of CD3 to the UXCD3 folder.
4. In the Jobs pane of the Deployment Console, select the job labelled **Run RemoteUX Driver Updates - UpdateXpress CD 1**. In the details pane of the Deployment Console select the **Run RemoteUX locally to update firmware** task and click **Modify**.

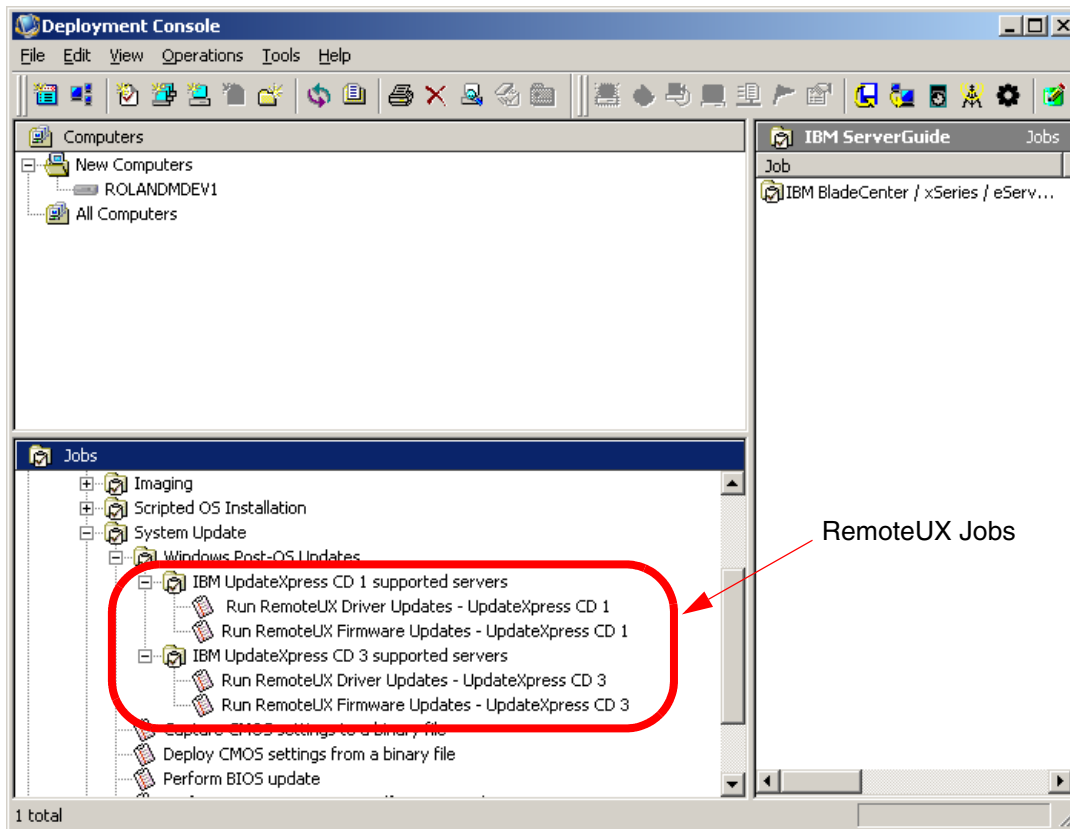


Figure 4-5 Deployment Console with the Run RemoteUX Drive Updates job's task highlighted

5. Scroll down the script until you see the line:

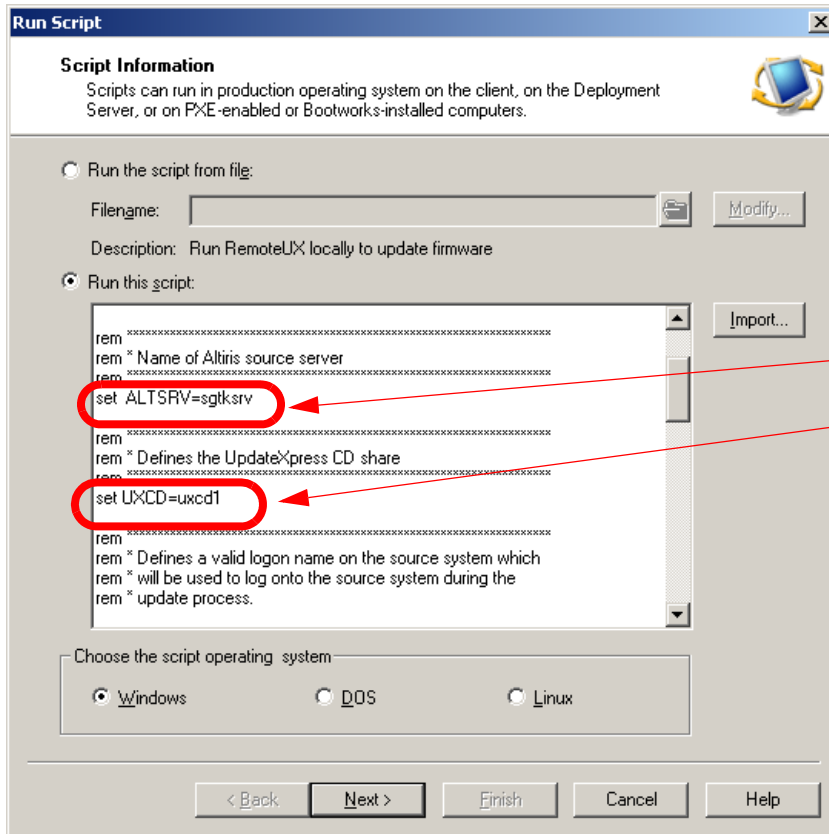
```
set ALTSRV=sgtksrv
```

Change the variable *sgtksrv* to match the hostname of the Deployment Server in your environment.

6. Next, continue scrolling down until you see the line:

```
set UXCD=uxcd1
```

Verify this path matches the path to the UpdateXpress CD1 content in the updates directory.



Change these variables to match your environment.

Figure 4-6 Variables that should be changed to match your environment

7. Next, continue scrolling down until you see the line:

```
set LOGON=sgtk0c1nt
```

Change the variable *sgtk0c1nt* to a user account name that has administrative privileges on the Deployment Server.

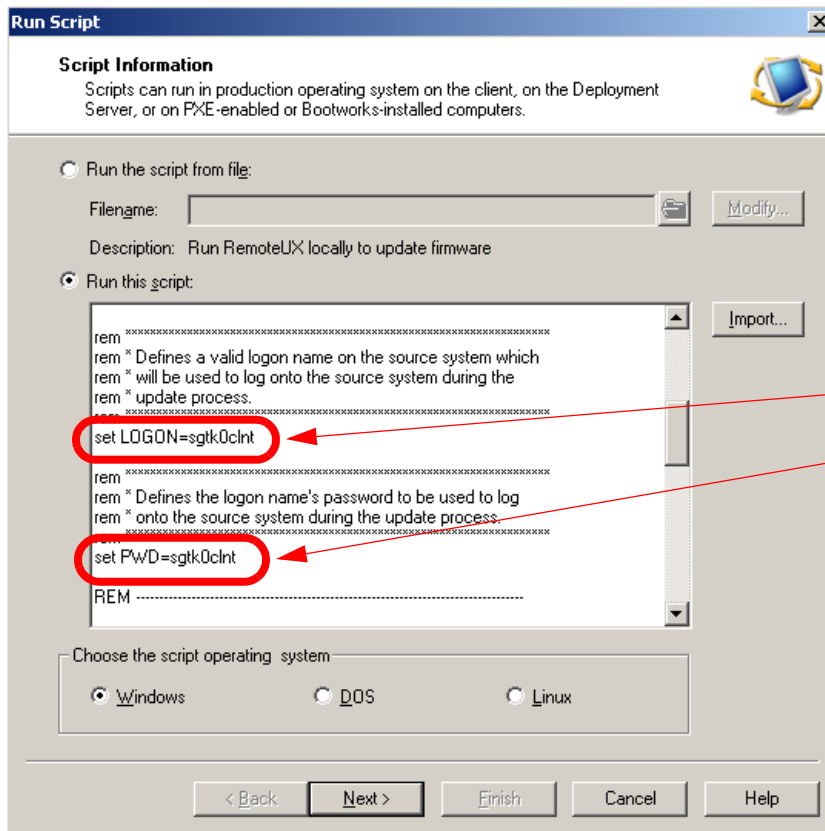
8. Next, continue scrolling down until you see the line:

```
set PWD=sgtk0c1nt
```

Change the variable *sgtk0c1nt* to the password for the user account that was entered in the previous step.

Important: The *LOGON* and *PWD* variables must match an administrator account on the Deployment Server or the job will fail. Also, the password cannot be blank.

Attention: The password used will be shown in clear text.



Change these variables to match your environment.

Figure 4-7 Variables that should be changed to match your environment

9. Click **Next** to continue to the next window.
10. Click **Next** to bypass the Script Details window and accept the default option to run the script on the client computer. Click **Finish** to complete customization of the **Run RemoteUX Driver Updates - UpdateXpress CD 1** job.
11. Repeat the process for the remaining RemoteUX jobs.

Table 4-4 on page 119 gives a complete listing of the user customizable variables in the RemoteUX jobs.

Table 4-4 Variables for the Run RemoteUX Firmware and Driver Updates jobs

Variable Name	Description	Defaults
ALTSRV	The hostname of the Altiris Deployment Server.	sgtksrv
UXCD	Defines the name of the shared folder which contains remoteux.exe utility and the necessary update files	uxcd1 (or uxcd3)
LOGON	Defines a user name that can log onto the Altiris source server during the update process. This user does not have to belong to the Administrator user group.	sgtk0clnt
PWD	The password of the account used for the LOGON variable. Note: The password cannot be empty.	sgtk0clnt

Deploying device drivers and firmware updates

When you have completed the integration of UpdateXpress with Altiris Deployment Solution as outlined above, the jobs are ready for deployment.

To update device drivers (for non-Blade computers), drag-and-drop the job labelled **Run RemoteUX Driver Updates - UpdateXpress CD 1** onto an active computer or group of computers in the Computers pane of the Deployment Console. For Blade computers, drag-and-drop the job labelled **Run RemoteUX Driver Updates - UpdateXpress CD 3** onto an active Blade computer or group of Blade computers.

Likewise, to update firmware (for non-Blade computers), drag-and-drop the job labelled **Run RemoteUX Firmware Updates - UpdateXpress CD 1** onto an active computer or group of computers in the Computers pane of the Deployment Console. For Blade computers, drag-and-drop the job labelled **Run RemoteUX Firmware Updates - UpdateXpress CD 3** onto an active Blade computer or group of Blade computers.

Managing system updates with UpdateXpress Server

UpdateXpress Server is a Web-based program for managing multiple versions of IBM device drivers and firmware updates from a central repository within your network. You can access the program on the server or remotely over any network that supports TCP/IP and Internet protocols.

You can use UpdateXpress Server to create system-specific profiles and associate them with the applicable device driver and firmware updates. Authorized users within your network can use a browser to access these profiles and download the applicable updates for their systems.

For more information about UpdateXpress Server go to the following IBM Web site:

http://www.ibm.com/servers/eserver/xseries/systems_management/uxsrv.html

4.2 Hardware configuration

As with keeping systems up-to-date, configuring hardware before provisioning can be a very time consuming and manual process. Altiris and IBM have included tools in Altiris Deployment Solution to make this process as painless as possible.

4.2.1 Configuring RAID

One of the most useful features added to Altiris Deployment Solution by the ServerGuide Scripting Toolkit is the ability to create policy-based RAID configurations on ServeRAID controllers offered in System x servers.

The ServerGuide Scripting Toolkit supports policy-based RAID configuration and replication using the PRAID.EXE utility. Some features of PRAID.EXE include:

- ▶ The ability to use the PRAID Policies file to describe how your RAID controllers should be configured or replicated.
- ▶ Customizable logic to determine the configuration to use with the many different controllers. This logic can include the machine type of the server, the number of drives connected to the controller, and the RAID controller type.
- ▶ An AUTO mode to configure using default settings.
- ▶ The ability to configure all RAID controllers in a system with a single program call.
- ▶ Features to capture useful information about each RAID configuration, including machine type, date, and time of capture.
- ▶ The ability to restore all controllers to factory-default settings.

In this section we will cover the PRAID Policies file used by the ServerGuide Scripting Toolkit to configure RAID, how to create a customized PRAID Policies file, and how to create new jobs in Altiris Deployment Solution to deploy the custom configuration.

Creating a PRAID Policies file

The ServerGuide Scripting Toolkit has a template Policies file that can be used to create custom RAID configurations for System x Servers. This section will

discuss how to leverage this template in creating your own powerful PRAID Policies files.

Follow the steps below to create a custom PRAID Policies file:

1. Open the Deployment Console.
2. Click **Tools** → **IBM Tools** → **IBM ServerGuide Scripting Toolkit Directory**. This will open the ServerGuide Scripting Toolkit source tree in Windows Explorer.
3. In Windows Explorer window navigate to directory “`. \sgdeploy\sgtk\examples\RAID\`”.

This directory contains the default template PRAID Policies files:

- The RAID-1-5 Policies file configures a RAID controller with a RAID-1 array using the first two drives, and a RAID-5 array using all remaining drives.
- The RAID5HSP Policies file configures a RAID controller with a RAID-5 array using all available drives and a single hot-spare drive.

There is also a template Policies file that can be customized to meet your needs.

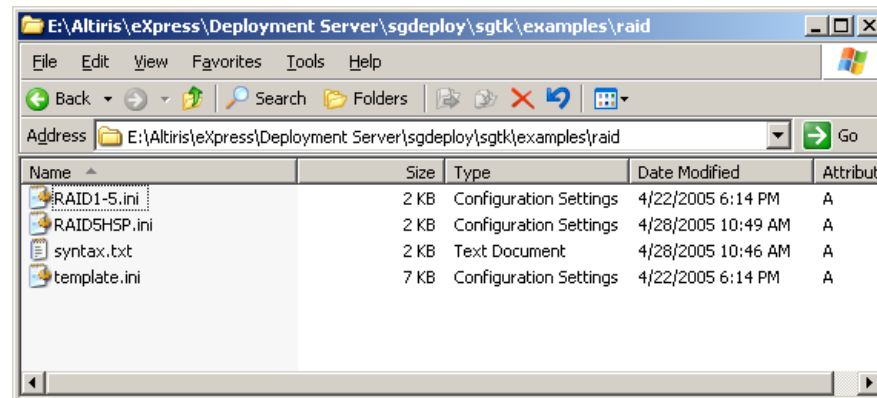


Figure 4-8 PRAID Policies files

4. Open the template.ini file in Notepad.

Table 4-5 on page 122 contains a brief explanation of the variables in the PRAID Policies file. For more information review the actual template Policies file, as it does a very good job of documenting each variable and its usage.

Table 4-5 Variables for the RAID policy file

Variable	Description and Syntax
[Policy.<name>]	<p>Labels the start of a policy, and gives the policy a name.</p> <p>Where: <name> is any combination of letters, numbers, underscores, dashes, or dots ('.').</p>
<p>AppliesTo.[n] = <parameter list></p> <p>Examples: AppliesTo.1 = t:ServeRAID-6M AppliesTo.2 = m:8870,s:56H3896</p>	<p>Tells when to use this policy. View the template policy file for a complete list of variables.</p> <p>Where: [n] is a number (1-12)</p> <p>Parameters: t:<controller_name> m:<machine_type> s:<machine_serial_number> c:<controller_number> (scan order relative to other RAID adapters) d:<number_of_drives_attached></p>
RebuildRate = <setting>	<p>Sets the controller rebuild rate. Default is HIGH.</p> <p>Where: <setting> is HIGH, MEDIUM, or LOW</p>
StripeSize = [n]	<p>Sets the controller stripe size. Default is 32.</p> <p>Where: [n] is 8, 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096</p>
ReadAhead = <setting>	<p>Sets the read-ahead caching mode for the controller. Default is ON.</p> <p>Where: <setting> is ON, OFF, or ADAPTIVE</p>
Array_Mode = <setting>	<p>Sets the mode to use when creating arrays. Default is AUTO.</p> <p>Where: <setting> is CUSTOM or AUTO</p>
<p>Array_Defaults = <variance>:<hotspares></p>	<p>Allows you to adjust the AUTO Array_Mode. Only valid if Array_Mode is set to AUTO.</p> <p>Where: <variance> is 0% (default), 5%, 10%, or 100%. <hotspares> is the number of hot-spare drives to create.</p>

Variable	Description and Syntax
<p>Array.[letter] = <drive_list></p> <p>Example: Array.A = 1,2 Array.B = 3,4 Array.C = ALL</p>	<p>Lists the drives to include in each array. Only valid if Array_Mode is set to CUSTOM. Use multiple entries to create more than one array.</p> <p>Where: [letter] is the array letter (A-H). <drive_list> is the list of drives to include in the array. May be listed by numerical order, by Channel/Target ID and SCSI/Bus num, or by using the keyword ALL to indicate all remaining drives should be used.</p>
<p>Hotspares = <drive_list></p> <p>Examples: Hotspares = 11,12 Hotspares = 1:11,1:12</p>	<p>Lists the drives to designate as hot-spare drives.</p> <p>Where: <drive_list> is the list of drives to designate as hot-spare drives. Drives may be listed by numerical order, by Channel/Target ID and SCSI/Bus num, or using the keyword ALL to indicate all remaining drives should be used.</p>
<p>Logical_Mode = <setting></p>	<p>Sets the mode to use when creating logical drives.</p> <p>Where: <setting> is AUTO or CUSTOM</p>
<p>Logical_Defaults = <size>:<RAID_level>:<write-cache_mode></p> <p>Example: Logical_Defaults = 4096:0</p>	<p>Allows you to adjust the AUTO Logical_Mode. Only valid if Logical_Mode is set to AUTO.</p> <p>Where: <size> is drive size in MB, or the keyword FILL. <RAID_level> is the RAID level for the logical drive (AUTO, 0, 1, 1E, 5, 5E, 5EE, etc.) <write-cache_mode> is ON, OFF, or AUTO.</p>
<p>Logical.[n] = <array_letter>:<size>:<RAID_level>:<write-cache_mode></p> <p>Examples: Logical.1 = A:FILL:1:ON Logical.2 = B:FILL:5</p>	<p>Lists the parameters to use when creating the logical drives. Only valid if Logical_Mode is set to CUSTOM.</p> <p>Where: <array_letter> is the letter of the array where the logical drive should be created (A-H). <size> is drive size in MB, or the keyword FILL. <RAID_level> is the RAID level for the logical drive (AUTO, 0, 1, 1E, 5, 5E, 5EE, etc.) <write-cache_mode> is ON, OFF, or AUTO.</p>

5. After reviewing the template file, close the template.ini file and open a new text document in Notepad.

For this example, we will use a System x3950 (x460) with a ServeRAID-8i controller and six SCSI hard disk drives. In our Policies file we will create two RAID-5 arrays each using three of the disk drives. We will then create two RAID-5 logical drives using the entire contents of each array. The completed PRAID Policies file is shown in Figure 4-9.

```
;Name the policy x460 RAID Level 5
[Policy.x460RL5]

;Make sure the policy will be used only for the ServeRAID 8i controller
AppliesTo.1 = t:ServeRAID-8i

;Accept the defaults for these values
RebuildRate = HIGH
StripeSize = 32
ReadAhead = ON

;Change this to CUSTOM to manually create our own arrays.
Array_Mode = CUSTOM

;We can skip Array_Defaults since it only applies to the AUTO setting.
;Here we create two arrays from the six disks.
;The parameter ALL uses all the remaining drives.
Array.A = 1,2,3
Array.B = ALL

;To create our logical drives manually, so we change the Logical_Mode to CUSTOM.
Logical_Mode = CUSTOM

;We skip Logical_Defaults since it only applies to the AUTO setting.
;Here we create two logical drives.
;The 1st creates a RAID 5 logical drive using the entire contents of Array A.
;The 2nd creates a RAID 5 logical drive using the entire contents of Array B.
Logical.1 = A:FILL:5
Logical.2 = B:FILL:5
```

Figure 4-9 The entire contents of a custom PRAID Policies file

6. Save and close the text document as X460RL5.ini in the raid folder.

Creating a custom RAID configuration job

Now that you have created a custom Policies file you can incorporate it into a custom RAID configuration job for later deployment.

Follow the steps below to create a custom RAID configuration job:

1. Open the Deployment Console and in the Jobs pane, navigate to **IBM BladeCenter / xSeries / eServer Support → Hardware Configuration**.

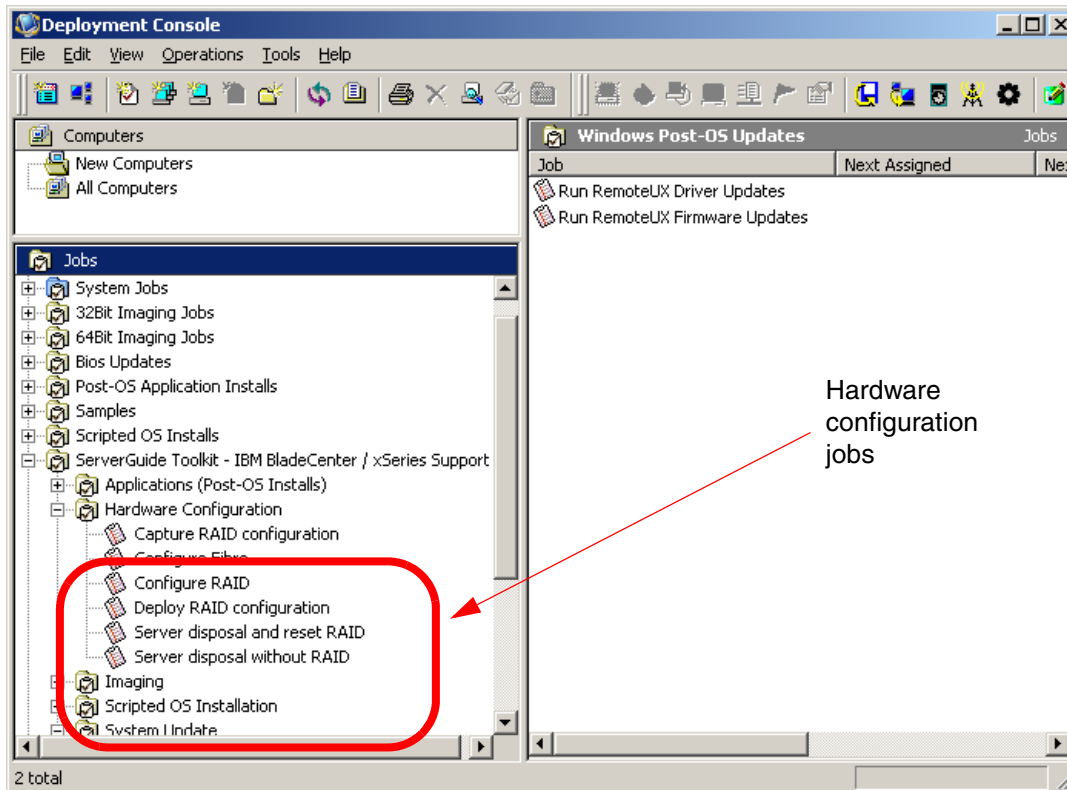


Figure 4-10 Deployment Console showing Hardware Configuration jobs

2. Right-click the job labelled **Configure RAID**. Select **Copy** from the pop-up menu to copy the job template to the clipboard.
3. Right-click in the Jobs pane and paste the Configure RAID job into the pane. This creates a copy of the original Configure RAID job template that can be customized to use the custom Policies file shown in Figure 4-9 on page 124.

4. Click the new **Configure RAID** job you just copied to the Jobs pane. The tasks included in the Configure RAID job will appear in the details pane of the Deployment Console.

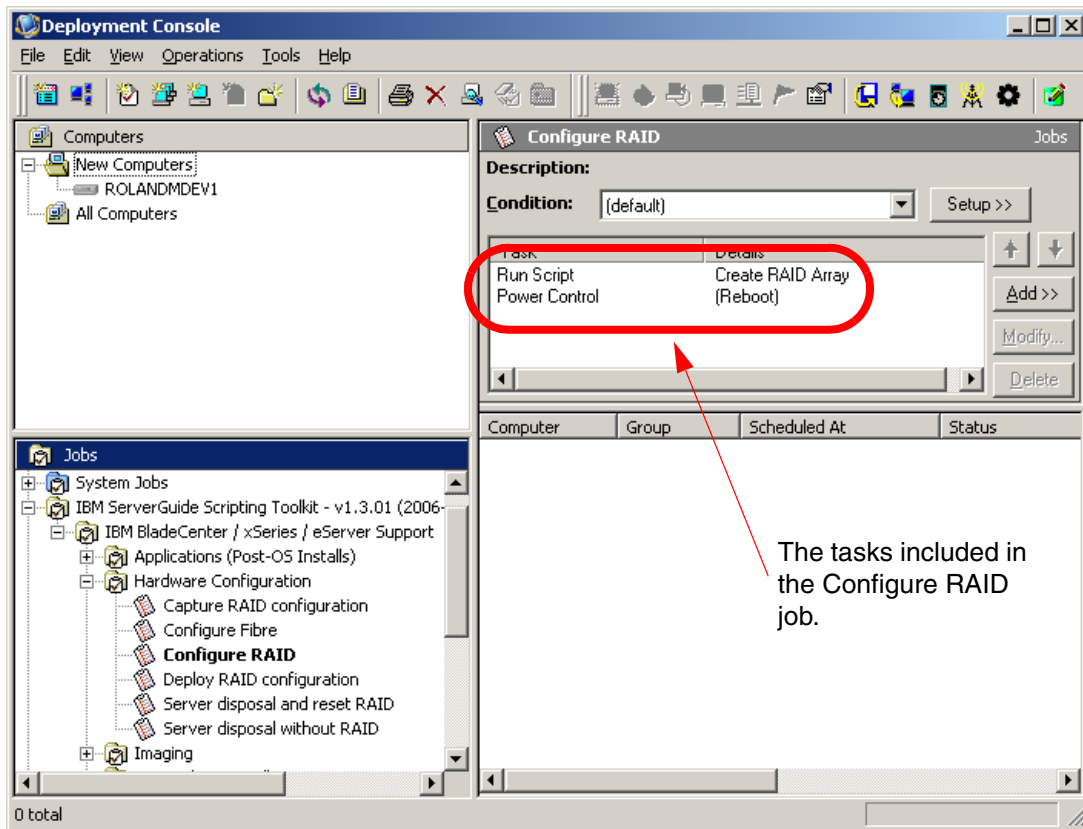
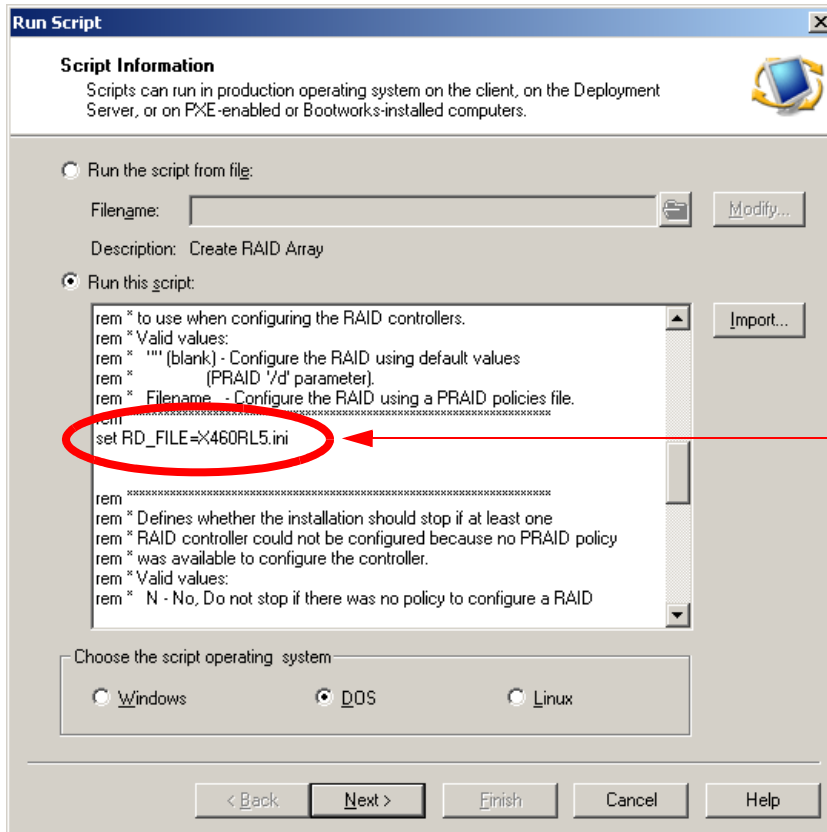


Figure 4-11 The tasks included in the Configure RAID job

5. Click the **Create RAID Array** task to enable the Modify button. Click **Modify** to open the Script Information window.
6. Scroll down the script until you find the line:
`set RD_FILE=`
Add the name of the new Policies file to the end of the line.



The name of your Policies file.

Figure 4-12 The Create RAID Array task with the name of the custom Policies file

7. Click **Next**. In the next window verify that the Automation - PXE or Bootworks Environment pull-down list has a PXE boot image that uses DOS. If Default Automation is selected, verify that Default Automation uses a DOS PXE boot image. Default Automation can be found on the DS tab of the PXE Configuration utility.

Important: The Configure RAID job requires a DOS environment. Do not use a Linux or Win PE PXE boot image.

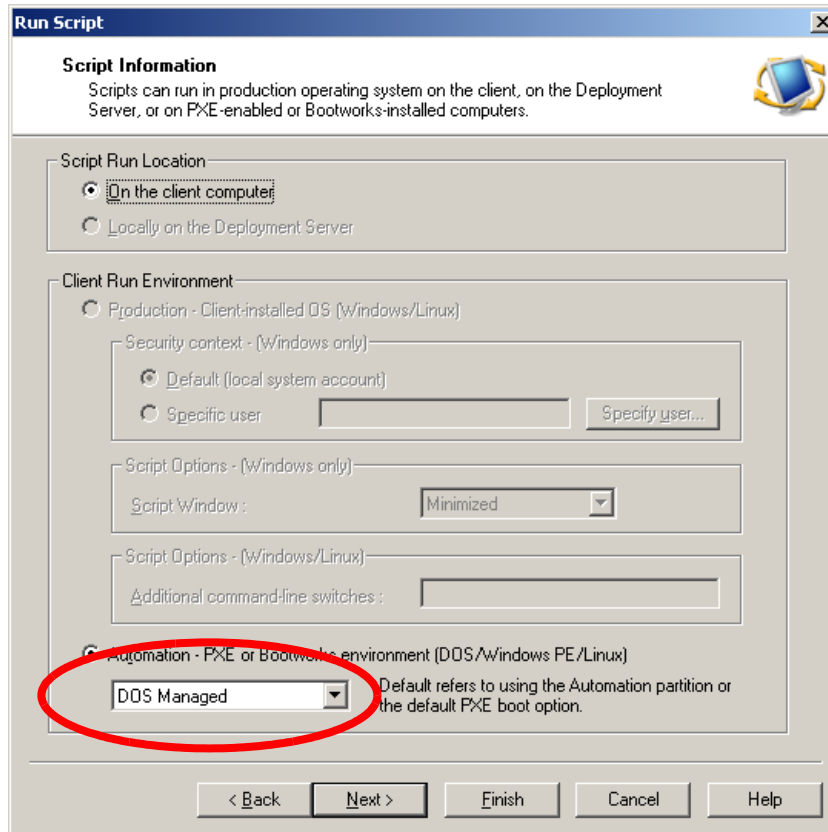


Figure 4-13 Verify a PXE boot image that uses DOS is selected in the pull-down list

- We do not want to create any custom return codes, so click **Next** and then click **Finish** to bypass the Return Codes window and return to the Deployment Console.

Note: If the custom Configure RAID job is run on a computer that does not have the ServeRAID 8i card installed, the job will fail and RAID will not be configured.

The custom Configure RAID job is ready to be deployed to a computer with a ServeRAID-8i installed. To deploy the job, drag-and-drop it from the Jobs pane onto an active computer or group of computers in the Computers pane.

If you want to further modify the Create RAID Array task in the Configure RAID job, the following table describes the customizable variables.

Table 4-6 Definitions for the variables in the Create RAID Array scrip

Variable	Description	Default
CFG_RD	Specifies whether to perform RAID configuration. Valid values are Y and N.	Y
RD_PATH	The fully qualified path to the RAID configuration files in the source tree.	%TK_PATH%\examples\raid (.\sgdeploy\sgtk\examples\raid)
RD_FILE	The name of the PRAID policies file. If no filename is specified, the RAID is configured using the default values.	No name specified
RD_ERR1	Indicates whether the installation should stop if at least 1 RAID controller cannot be configured because no policy is available. Valid values are: N - do not stop the installation Y - stop the installation	N
RD_ERR2	Indicates whether the installation should stop if no supported RAID controllers are found in the system. Valid values are: N - do not stop the installation Y - stop the installation	N

4.2.2 Configuring a Fibre Channel HBA for boot from SAN

In addition to the ability to configure RAID, Altiris Deployment Solution has been provided the ability to configure Fibre Channel HBAs to boot from SAN through the integration of the ServerGuide Scripting Toolkit.

In this section we cover the creation of a custom Configure Fibre job.

Note: The current release of the IBM ServerGuide Scripting Toolkit supports only QLogic host bus adapters.

Creating a custom Configure Fibre job

This section covers the creation of a custom Fibre Channel configuration job. In most cases accepting the defaults works fine. However, when running the job on a target computer that is installed with multiple QLogic HBAs you will need to customize the job tasks to point to the HBA you want to use with the storage device. For instructions on how to do this see “Obtaining the Fibre Channel adapter’s I/O address and WWN (optional)” on page 134.

Follow the steps below to create a custom Fibre Configuration job:

1. Open the Deployment Console and in the Jobs pane, navigate to folder **IBM BladeCenter / xSeries / eServer Support** → **Hardware Configuration**.

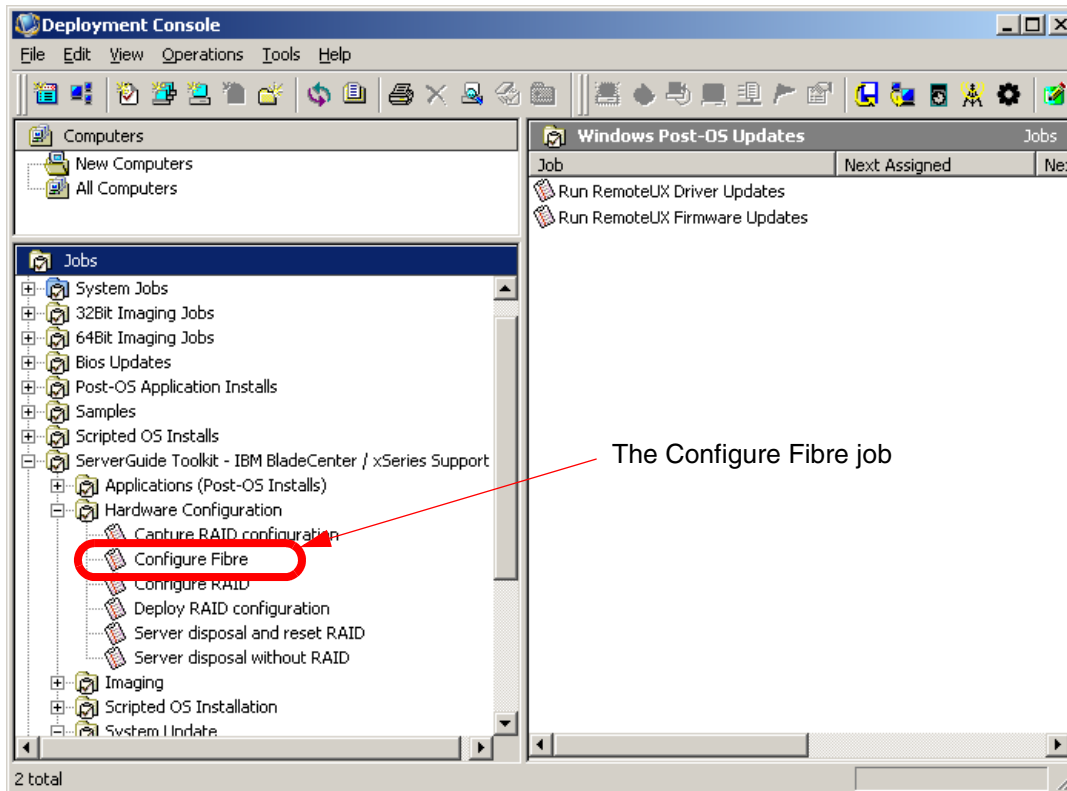


Figure 4-14 Deployment Console showing the Fibre Configuration job

2. Right-click the job labelled **Configure Fibre** and click **Copy** to copy the job template to the clipboard.
3. Right-click in the Jobs pane and paste the Configure Fibre job into the pane. This creates a copy of the original Configure Fibre job template that can be customized without overwriting the original job.
4. Click the new **Configure Fibre** job you just copied to the Jobs pane. The tasks included in the configure Fibre job will appear in the details pane of the Deployment Console.

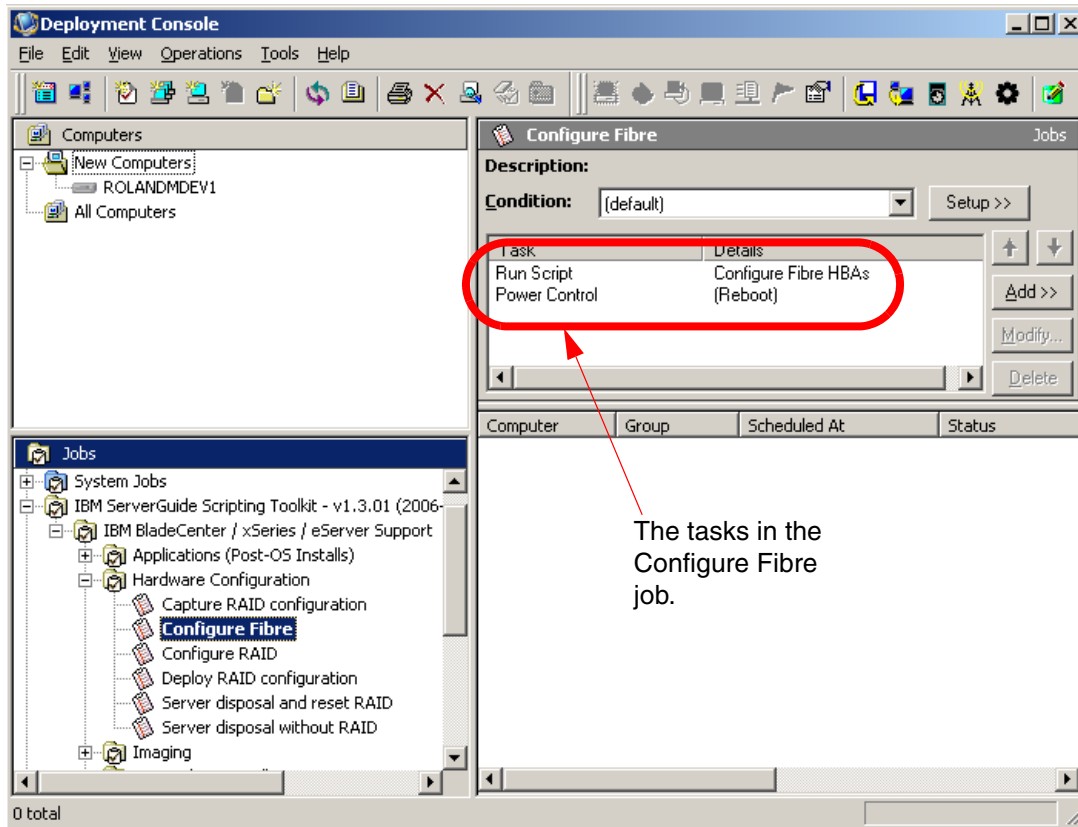


Figure 4-15 The Configure Fibre job's tasks

5. Select the **Configure Fibre HBAs** task and click **Modify** to open the task in edit mode.

6. Scroll down the script until you find the line:

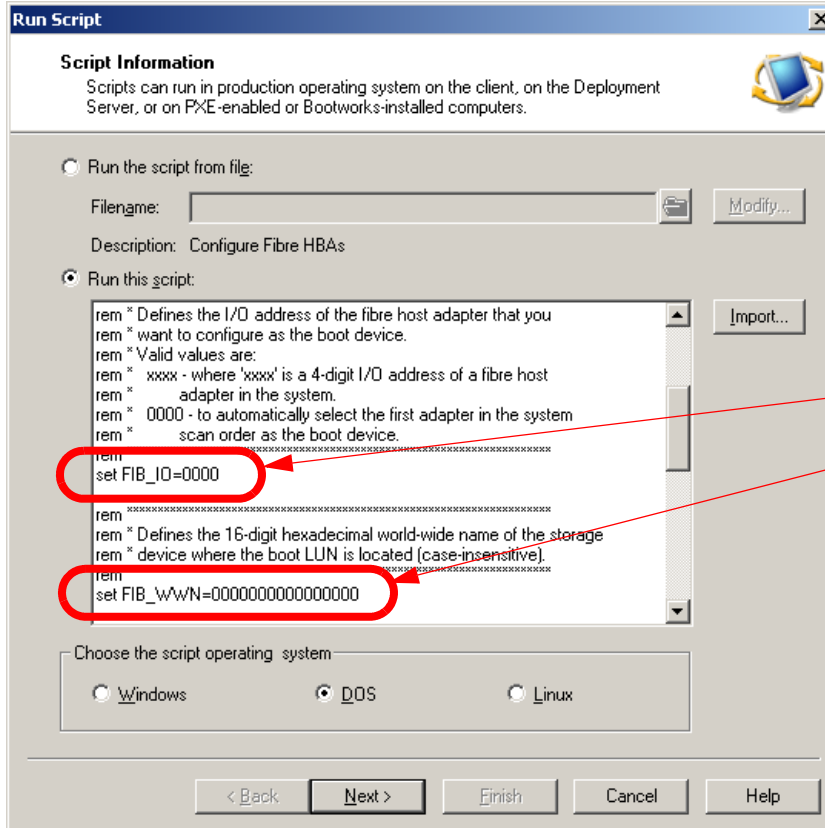
```
set FIB_IO=0000
```

This line defines the I/O address of the HBA to configure. Setting FIB_IO to the default value of **0000** will cause the first adapter in the system scan order to be configured. The first adapter in the system scan order is the one with the lowest I/O address. If you require more control over which adapter to configure (for example you have more than one HBA installed in the server), you can change this to match the I/O address of the correct adapter. For an overview on how to do this see "Obtaining the Fibre Channel adapter's I/O address and WWN (optional)" on page 134.

7. Scroll down the script until you find the line:

```
set FIB_WWN=0000000000000000
```

This line defines the 16-digit hexadecimal world-wide name of the storage device where the boot LUN is located. If you keep the default of all zeros, the HBA with the lowest WWN will be used as it will be the first one found. Again, this can be changed for more control. See “Obtaining the Fibre Channel adapter’s I/O address and WWN (optional)” on page 134 for information about obtaining the HBA’s WWN.



Script variables for the HBA’s I/O address and World-wide name.

Figure 4-16 The Configure Fibre HBAs script

8. Continue to scroll down the script until you locate this line:

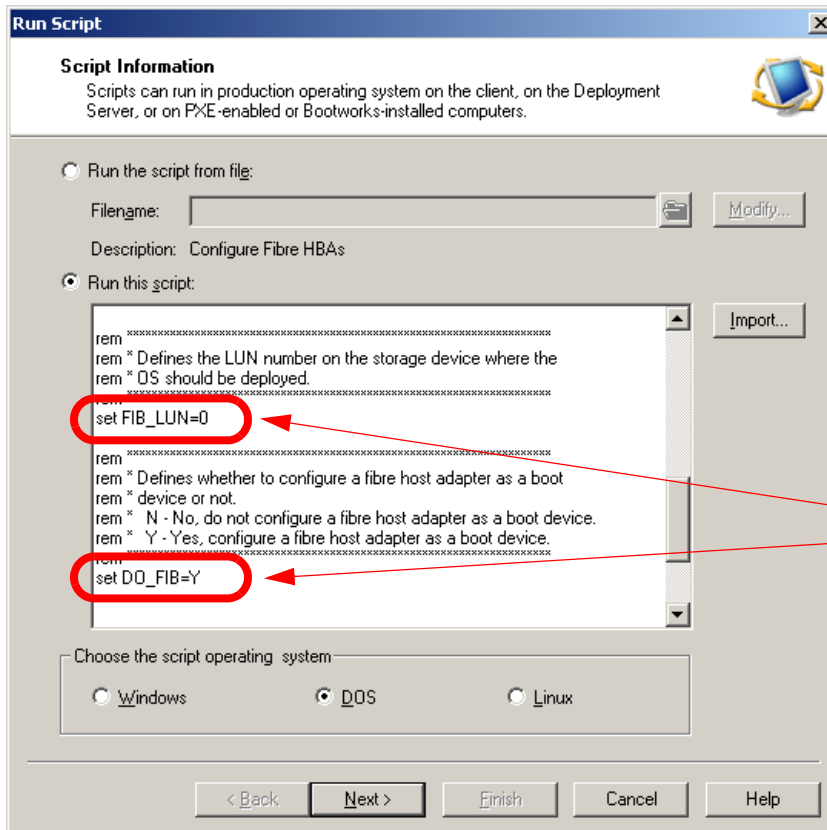
```
set FIB_LUN=0
```

This variable defines the LUN number on the storage device where the operating system should be deployed. Default value is “0”. If you want to point to a different LUN, change this to the correct LUN number for your environment. If you leave this as the default, the LUN with the lowest loop ID will be used as the boot device, as it will be the first one found.

9. Scroll down the script until you locate this line:

```
set DO_FIB=Y
```

This variable defines whether to configure a fibre host adapter as a boot device or not. If you would rather not have the computer boot to the LUN change this variable to N.



Script variables for the LUN Number and boot to Fibre Channel.

Figure 4-17 The Configure Fibre HBAs script (continued)

10. The customization is finished for this task. Click **Next** to continue.

11. Click **Next**. In the next window verify that the Automation - PXE or Bootworks Environment pull-down list has a PXE boot image that uses DOS. If Default Automation is selected, verify Default Automation uses a DOS PXE boot image. Default Automation can be found on the DS tab of the PXE Configuration utility.

Important: The Configure Fibre job requires a DOS environment. Do not use a Linux or Win PE PXE boot image.

12. Click **Finish** to complete the process.

The custom **Configure Fibre** job is ready for deployment. To deploy the job, drag-and-drop it from the Jobs pane onto an active computer or group of computers in the Computers pane.

Obtaining the Fibre Channel adapter's I/O address and WWN (optional)

In most cases you do not need the I/O address or the WWN name of the HBA to create a custom job in Altiris Deployment Solution. If you have only one QLogic host bus adapter installed in the computer the defaults are typically fine. However, for more advanced setups you may want to specify the exact I/O address and WWN of your HBA.

By default the first HBA in the computer scan order will be selected. The first adapter in the system scan order is the one with the lowest I/O address.

Both the I/O address and the WWN name of the HBA can be obtained in the QLogic Fast!UTIL application.

To open the QLogic Fast!UTIL application follow the steps below:

1. Power on the server installed with the QLogic adapter.
2. To enter the QLogic Fast!UTIL application, press the key combination Ctrl+q when prompted during POST.

For more information about QLogic host bus adapters visit the QLogic Web site at the following URL:

<http://www.qlogic.com>

4.2.3 Capturing and deploying RAID configurations

The IBM ServerGuide Scripting Toolkit provides Altiris Deployment Solution with jobs to capture and deploy RAID configurations on IBM BladeCenter or System x Servers. The jobs, which are installed with the ServerGuide Scripting Toolkit, are labelled Capture RAID configuration and Deploy RAID configuration. They can be found in the Jobs pane of the Deployment Console by navigating to folder **IBM BladeCenter / xSeries / eServer Support** → **Hardware Configuration**.

The Capture RAID configuration and Deploy RAID configuration jobs can be used to take a snapshot of a computer's current RAID configuration and to later deploy those settings to other computers of the same machine type, installed with the same number of hard disk drives attached to the same type of RAID controller as the Reference Computer.

Capturing RAID configurations

When run on a Reference Computer, the **Capture RAID Configuration** job determines how PRAID would configure the reference RAID controller and creates a Policies file documenting the current RAID configuration of the Reference Computer. The Policies file is saved as `raidclon.ini` in the folder `“.\sgdeploy\altiris\temp\MachineType\”` in the ServerGuide Scripting Toolkit source tree.

Deploying RAID configurations

When deployed to an active computer or group of computers, the job labelled Deploy RAID Configuration looks in the aforementioned directory, with *MachineType* being the machine type of the target computer, for the file named `raidclon.ini`. If the file is located, the job will configure the target computer's RAID controller.

Note: The target computers must have the same number of hard disk drives attached to the same type of controller as the Reference Computer.

4.2.4 Server disposal and reset RAID

In a world where the protection of secure data is increasingly important, tools for server disposal have become a required tool in many business environments. The IBM ServerGuide Scripting Toolkit provides Altiris Deployment Solution with jobs to dispose of secure data fast and efficiently. The jobs, which are installed with the ServerGuide Scripting Toolkit, are:

- ▶ Server disposal and reset RAID
- ▶ Server disposal without RAID

These jobs can be found in the Jobs pane of the Deployment Console in **IBM BladeCenter / xSeries / eServer Support** → **Hardware Configuration**.

The Server disposal and reset RAID job is a very powerful tool. It allows you to perform secure data disposal on IBM BladeCenter or IBM System x servers. The job performs the following tasks:

- ▶ Erase data from one or all hard disks that are connected to the target computer
- ▶ Reset supported RAID controllers and adapters in the target computer to factory-default settings
- ▶ Delete all partitions on hard disks that are connected to the target computer

The Server disposal and reset RAID job has many customizable options to ensure your data is securely disposed. Modify the job's tasks as was described earlier in "Creating a custom RAID configuration job" on page 125.

The disposal job uses the scrub3.exe utility to clean the disk of data. The scrub3 utility allows you to specify the level of clean-up on the command-line. You specify the level in the job by modifying the SL parameter, as follows:

```
set SL=x
```

Where x can be 1, 2, 3 or 4:

- 1 = Limited security. The MBR and some sectors are overwritten once
- 2 = Medium security. All sectors are overwritten once
- 3 = High security. All sectors are overwritten four times
- 4 = US Department of Defense-compliant security. All sectors are overwritten seven times.

For further customization of the Server disposal - Erase hard disk drives script, see Table 4-7.

Table 4-7 Definitions for the variables in the Server disposal

Variable	Description	Default
DRV_NUM	Defines the drive number to erase. Valid values: ALL - To erase all hard disk drives in the system "n" - To erase the "n"th drive, where n is a positive integer.	ALL
SMETH	Defines which scrub method to use to erase the drives. These values are mutually exclusive. Valid values: 1 - Use the security level environment variable (SL) 2 - Use the write level environment variable (SW)	1

Variable	Description	Default
SL	Defines the desired level of security when cleaning the drive(s). Valid values: 1 - Limited security: The master boot record & some sectors are overwritten once. 2 - Medium security: All sectors are overwritten once. 3 - High security: All sectors are overwritten 4 times. 4 - US Department of Defense compliant security: All sectors are overwritten 7 times.	1
SW	Defines using the number of times each sector is overwritten. The value supplied must be a positive integer (2 - 99).	2
SSIG	Defines whether to write the Scrub signature to the drive or not. Valid values are: N - No, do not write the Scrub signature. Y - Yes, write the Scrub signature.	N

The final script in the Server disposal and reset RAID job, labelled Server disposal - Reset RAID array, resets the RAID controller to default settings and removes all partitions on the target computer's hard disk drives.

The second job devoted to server disposal, labelled Server disposal without RAID, is exactly the same as the first job, except the last script for resetting the RAID controller to default settings is not included.

The Server disposal without RAID job can be configured the same as the Server disposal and reset RAID job. For a listing of customizable variables see Table 4-7 on page 136.

To deploy the server disposal jobs, drag-and-drop them from the Jobs pane onto an active computer or group of computers in the Computers pane.



Using script-based deployment

Script-based deployment is a method of deployment that performs an unattended installation of an operating system. During the installation process, script-based deployment uses an answer file (or a kickstart file when scripting Linux) in replace of user interaction.

This chapter covers the basics of script-based deployment of both Microsoft Windows and Red Hat Linux.

The following topics are discussed:

- ▶ 5.1, “Script-based deployment versus image-based deployment” on page 140
- ▶ 5.2, “Script-based deployment of Windows and Linux” on page 140
- ▶ 5.3, “Deploying VMware ESX Server 2.5” on page 157

5.1 Script-based deployment versus image-based deployment

Script-based deployment is simply an unattended operating system installation using an answer file to replace user interaction during the install process. Image-based deployment is creating an image of a computer's hard drive and copying that image onto other machines, creating clones of the original. Image deployment is covered in greater detail in Chapter 6, "Using image-based deployment" on page 167.

Script-based deployment has a few advantages over image-based deployment:

- ▶ Saves time by not having to manage and update operating system images
- ▶ Easier to implement and manage within Altiris Deployment Solution
- ▶ Does not require a reference computer for creation of a donor image

The downfall to script-based deployment is:

- ▶ Script-based deployment takes longer than image-based deployment because a scripted install is actually performing a native installation of the operating system.

5.2 Script-based deployment of Windows and Linux

The ServerGuide Scripting Toolkit provides Altiris Deployment Solution with a number of scripted install sample jobs for Windows 2000, Windows Server 2003, multiple versions of Red Hat Enterprise Linux, and SUSE Linux. The jobs, which are installed with the ServerGuide Scripting Toolkit, can be found in the Jobs pane of the Deployment Console, in the folder IBM BladeCenter / xSeries / eServer Support → System Update

Note: The folder named **IBM BladeCenter / xSeries / eServer Support** is in the Jobs pane of the Deployment Console inside folder "IBM ServerGuide Scripting Toolkit - *version_number (release_date)*", where *version_number* is the version of the ServerGuide Scripting Toolkit on which the IBM jobs are based and *release_date* is the date this version was released.

When a new version of the ServerGuide Scripting Toolkit is released and installed, new jobs are added to the Deployment Console. The jobs are added in a new folder to negate the possibility of overwriting any customized jobs from previous versions of the ServerGuide Scripting Toolkit.

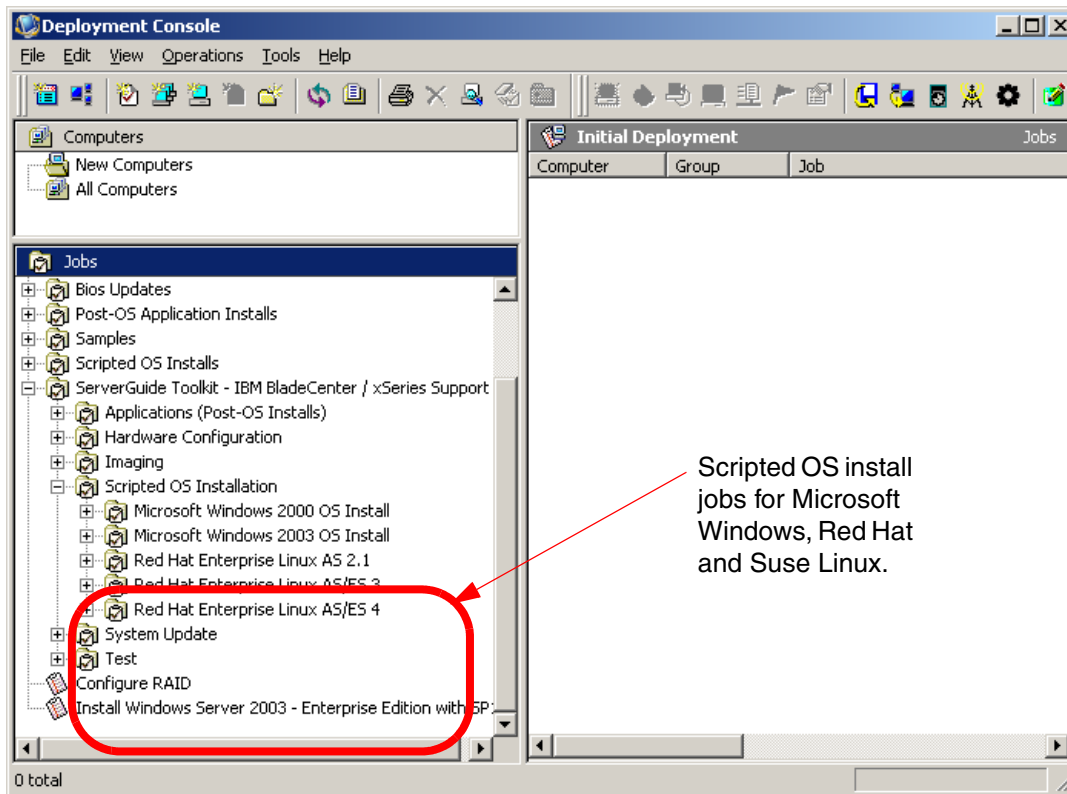


Figure 5-1 The Deployment Console with containers housing scripted installation jobs

To prepare for Script-based deployment the following requirements need to be met:

- ▶ The installation media must be copied to the ServerGuide Scripting Toolkit source tree
- ▶ The device drivers must be copied to the ServerGuide Scripting Toolkit source tree (Windows only)
- ▶ The task scripts for the scripted install jobs must be altered to:
 - Point to the directory housing the installation media
 - Point to the directory housing the answer/kickstart file
 - Point to the directory housing the device drivers (Windows only)
- ▶ Microsoft IIS must be installed on the Deployment Server and, for Linux installs, a virtual directory must be created

In this chapter we will cover the creation of a Windows answer file, the creation of a Red Hat Linux kickstart file, the creation of customized jobs for deploying both Windows and Linux, and the creation of a virtual directory in Microsoft IIS.

5.2.1 Integrating operating system installation media and device drivers

Before deploying a Windows or Linux scripted install, Altiris Deployment Solution must have the operating system installation media and device drivers (device drivers are required for Windows only) copied to the deployment share. The ServerGuide Scripting Toolkit makes this process very quick and easy through the Toolkit Configuration Utility.

To read more about the Toolkit Configuration Utility and loading operating system installation media and device drivers see 2.2.2, “Configuring the ServerGuide Scripting Toolkit source tree” on page 35.

5.2.2 Preparing a Windows answer file

Before deploying a scripted install job to one or more target computers, you must customize an answer file for Windows Setup to use when installing the operating system.

Follow the steps below to create an answer file for a Windows 2003 with SP1 scripted install:

1. Open the Deployment Console.
2. Open the ServerGuide Scripting Toolkit source tree by clicking **Tools** → **IBM Tools** → **IBM ServerGuide Scripting Toolkit directory** on the main menu.

The operating system answer files are saved in directory
.\sgdeploy\sgtk\altiris\windows\ansfiles

3. By default the folder contains two answer files:
 - win2000.txt — a template for Windows 2000
 - win2003.txt — a template for Windows Server 2003

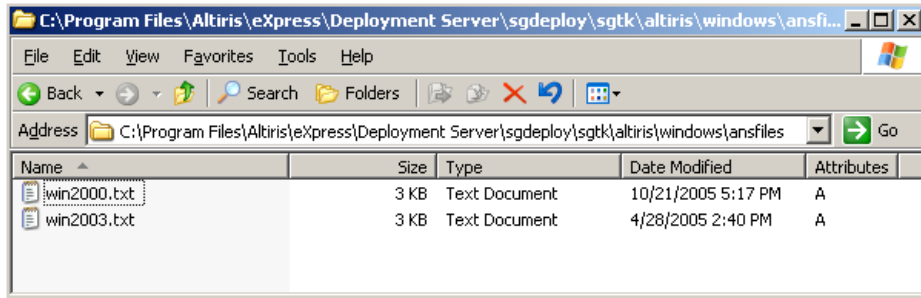


Figure 5-2 Windows answer files

- Open in Notepad the win2003.txt file.

Note: For a complete listing of variables and how they are used in Windows answer files reference the following URL:

<http://www.microsoft.com/technet/prodtechnol/Windows2000Pro/deploy/unattend/sp1ch01.mspx>

- Scroll down to the first section in the answer file, labeled [MassStorageDrivers]. This section allows the addition of SCSI and other mass-storage drivers that are not included with the Windows 2003 install media. Refer to the URL mentioned above for syntax regarding this section.
- Scroll down the answer file until you find the [Unattended] section. Locate the variable shown here:

```
;ExtendOemPartition = 1
```

The ExtendOemPartition variable controls the size of the partition on the Target Computer's hard disk. Notice the variable is preceded by a semi-colon. If the semi-colon is not removed, this variable will be ignored. However, we do not want this line ignored so remove the semi-colon. The value of 1 tells Windows Setup to extend the partition to fill out the hard disk on the Target Computer.

```
[Unattended]
UnattendMode = FullUnattended
OemPreinstall = Yes
DriverSigningPolicy = Ignore
OemFilesPath =
OemPnPDriversPath =
OemSkipEula = Yes
FileSystem = ConvertNTFS
ExtendOemPartition = 1
```

Figure 5-3 Our [Unattended] section

Tip: You can add a variable in the [Unattended] section named `ComputerType` that will recognize computers with different hardware abstraction layers (HALs) and will load the correct HAL. This is especially useful for servers like the x445 that requires a special HAL. For more information about this variable and syntax see the following URL:

<http://www.microsoft.com/technet/prodtechnol/Windows2000Pro/deploy/unattend/sp1ch01.mspx>

7. Scroll down to the [UserData] section. Notice the variables `FullName` and `ComputerName` use tokens (surrounded by a percent sign, %). These tokens are supplied by Altiris Deployment Solution in one of the later tasks in the Scripted Install job. If you do not want to use tokens, change the variables to something more appropriate for your environment.

The last variable in this section, labeled `ProductID`, has also been preceded with a semi-colon. If you want Windows Setup to automatically add the Windows Product ID key, remove the semi-colon and type your Windows Product ID key.

```
[UserData]
FullName = "%NAME%"
OrgName = "Company"
ComputerName = "%COMPNAME%"
;ProductID = "11111-11111-11111-11111-11111"
```

Figure 5-4 The [UserData] section before being updated

8. Scroll down to the [GuiUnattended] section. Locate the variable shown here:
`AdminPassword = *`

The AdminPassword variable creates the Administrator password in Windows. The asterisk creates a blank password. If you want to change this, type in a password surrounded by quotation marks.

Note: If you enter a password into an answer file it will be shown in clear text and readable by any user with the right to access the deployment share.

9. Scroll down to the [Components] section which allows you to turn various Windows components on and off during Windows Setup.

If you want to include a Windows component, change the variable setting to ON. Conversely, change the variable setting to OFF if you do not want it to be included in the Windows install.

10. When you have finished making changes to the answer file, close and save the text file.

5.2.3 Creating a Windows Scripted Install job

When you have copied the operating system installation media and device drivers to the ServerGuide Scripting Toolkit source tree and created an answer file, you can edit the scripted install job task to point to the directories housing the installation media, device drivers, and answer file. However, before altering the job, make a copy to edit so the original template job is not overwritten.

In the following examples we will create a scripted install job for Windows 2003 with integrated SP1. Follow the steps below to create a custom job:

1. Open the Deployment Console.
2. In the Jobs pane, explore to the following folder: IBM ServerGuide Scripting Toolkit - *version (release_date)* → IBM BladeCenter / xSeries / eServer Support → Scripted OS Installation as shown in Figure 5-5 on page 146. In this folder are a number of other folders that contain the jobs for each version of supported operating systems.
3. Expand the folder **Microsoft Windows 2003 OS Install** as shown.

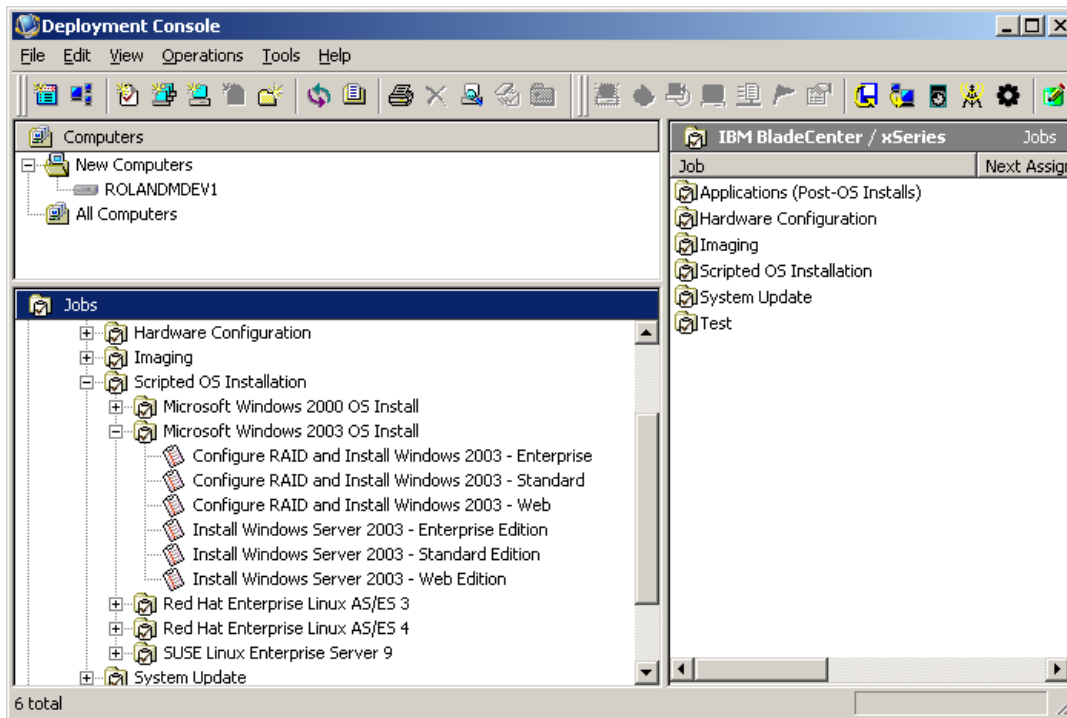


Figure 5-5 Deployment Console with the Microsoft Windows 2003 Scripted OS install jobs

4. Right-click the job labelled **Install Windows Server 2003 - Enterprise Edition** and select **Copy** from the pop-up menu.
5. Right-click an area in the Jobs pane and select **Paste** from the pop-up menu. Now you can alter the tasks in this job without overwriting the original job template.
6. Select the job you just copied and in the details pane select the task named **Customize Windows 2003 Variables**. Now click **Modify** to open the task in edit mode.

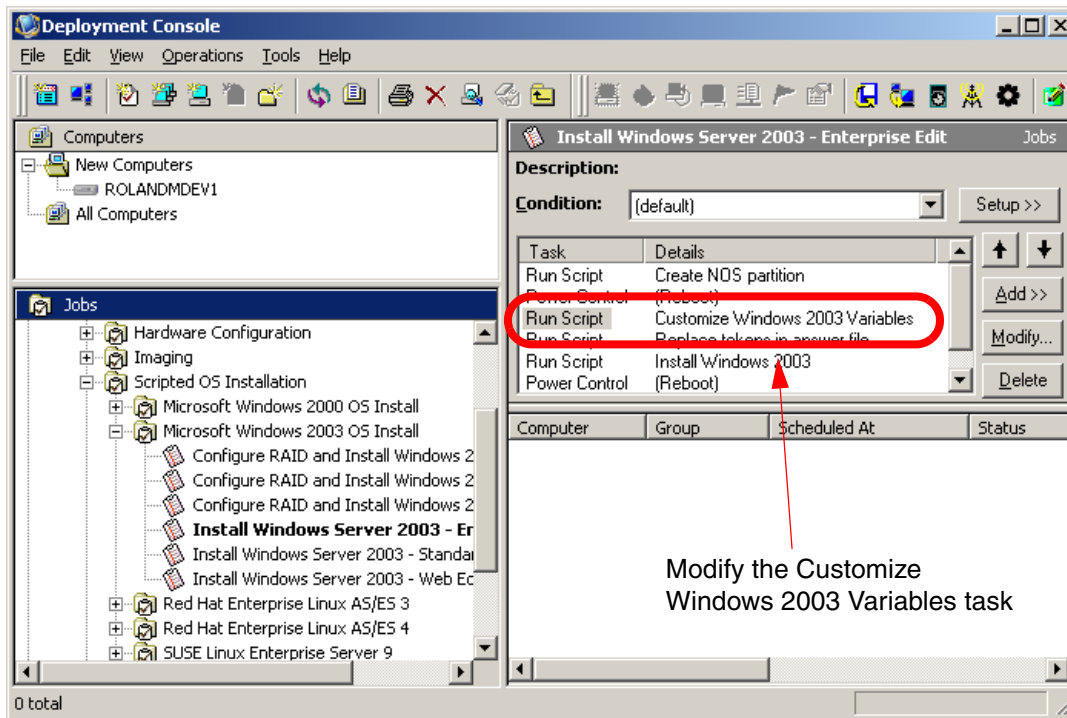


Figure 5-6 Deployment Console with the tasks for a Windows scripted OS install job

7. Scroll down the script until you locate the following variable:

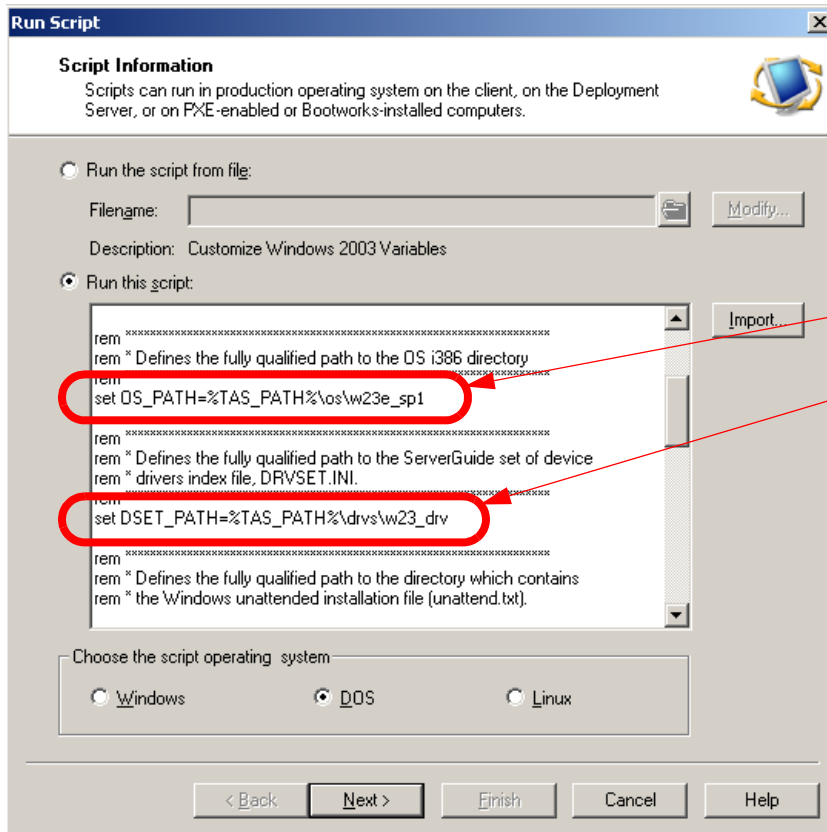
```
set OS_PATH=%TAS_PATH%\os\w23_ent
```

Change the path to match your environment. In our test environment we installed the Windows 2003 installation media to the default directory (w23_ent) so no change was required.

8. Scroll down the script until you locate the following variable:

```
set DSET_PATH=%TAS_PATH%\drvs\w23_drv
```

Change the path to match your environment. In our test environment we installed the Windows 2003 device drivers to the default directory (w23_drv) so no change was required.

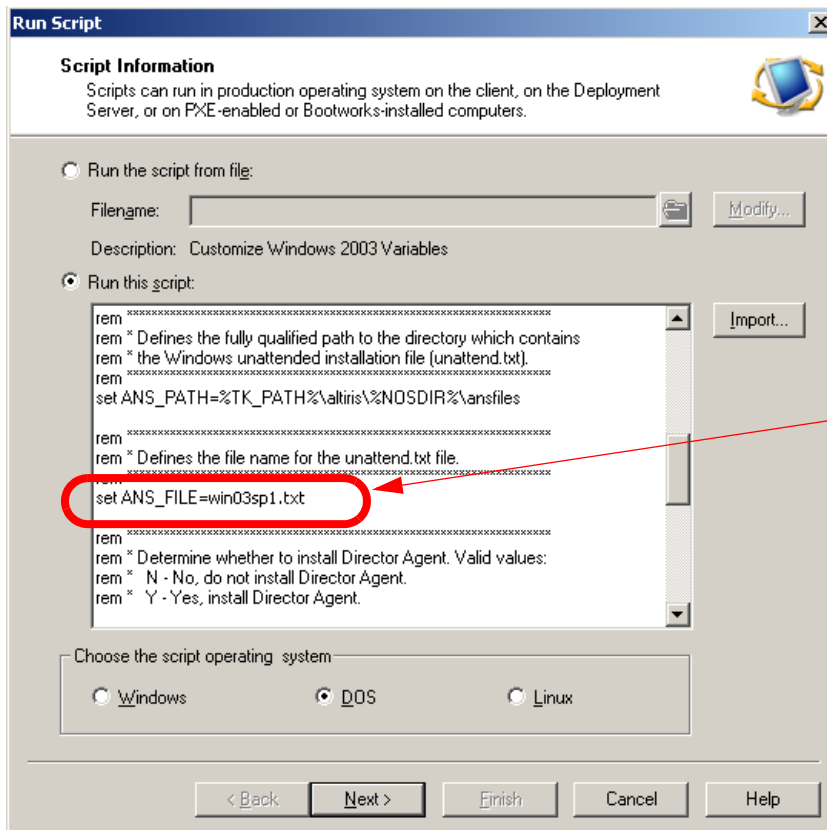


Make sure these paths are correct for your environment

Figure 5-7 The Customize Windows 2003 Variables task after changes have been made

9. Scroll down the script until you locate the following variable:
`set ANS_FILE=win2003.txt`

Change the path to point to your custom answer file. In our case we are using the answer file we edited above, named win2003.txt so no change was required.



Make sure this path is correct for your environment

Figure 5-8 The Customize Windows 2003 Variables task after changes have been made

10. After making the required changes, click **Next** to continue.

11. Click **Finish** on the Script Information window to close the task editor.

The custom job for deploying a scripted installation of Windows Server 2003 is complete.

Drag the job you created onto an active computer or group of computers in the Computer pane of the Deployment Console to deploy a scripted installation of Windows Server 2003.

5.2.4 Configuring HTTP and FTP for Linux scripted installations

Linux uses a different method than Microsoft uses for transferring operating system installation files to the target computer. Linux requires an FTP server to serve the operating system installation files.

To deploy a scripted installation of Linux you must first install Microsoft IIS on your Deployment Server. This document assumes a working knowledge of Microsoft IIS.

When you have installed IIS, create a new virtual directory. Enter **sgdeploy** as the alias for the virtual directory and point it to the ServerGuide Scripting Toolkit source tree (the sgdeploy directory in the Deployment Share). Allow Read (default) and Browse permissions by checking the appropriate check boxes.

When you have created the virtual directory you need to change the MIME Types of the directory. Follow the steps below to change the MIME Types:

1. Right-click the **sgdeploy** virtual directory and select **Properties** from the pop-up menu.
2. Click the **HTTP Headers** tab.

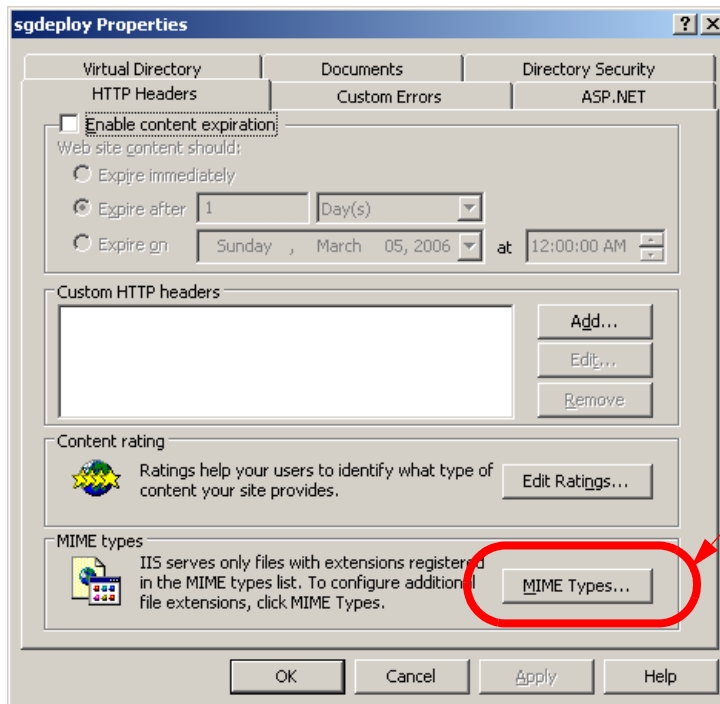


Figure 5-9 The Properties window for the sgdeploy virtual directory in Microsoft IIS

3. Click **MIME Types** in the MIME Types section.
4. Click **New**.
5. In the first text box, type `.*` and in the second text box, type `application/octet-stream`.

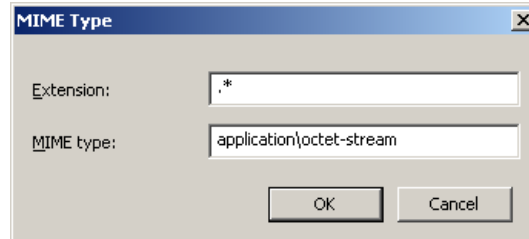


Figure 5-10 The MIME Type window with added text

6. Click **OK**.
7. Click **OK** again to close the Properties window.

The IIS configuration is now complete. When the Linux scripted installation is initiated the Target Computer(s) will download the installation media from the virtual directory.

5.2.5 Preparing a Linux kickstart file

Before deploying a scripted installation job to one or more target computers, you must customize a kickstart file (the Linux version of an answer file) for Linux Setup to use when installing the operating system.

Note: For more information about kickstart files refer to Red Hat official documentation at the following URL:

<http://www.redhat.com/docs/manuals/linux/>

Follow the steps below to create a kickstart file for a Red Hat Enterprise Linux 3 scripted installation:

1. Open the Deployment Console.
2. Open the ServerGuide Scripting Toolkit source tree by clicking **Tools** → **IBM Tools** → **IBM ServerGuide Scripting Toolkit directory** on the main menu.
3. The Red Hat Linux kickstart files are saved in directory `.\sgdeploy\sgtk\altiris\linux\redhat`

4. By default the folder contains eight answer files for each of the versions of Red Hat supported by the ServerGuide Scripting Toolkit.
5. Copy and paste the rhes3ks.cfg file into the same directory and rename it rhes3new.cfg.

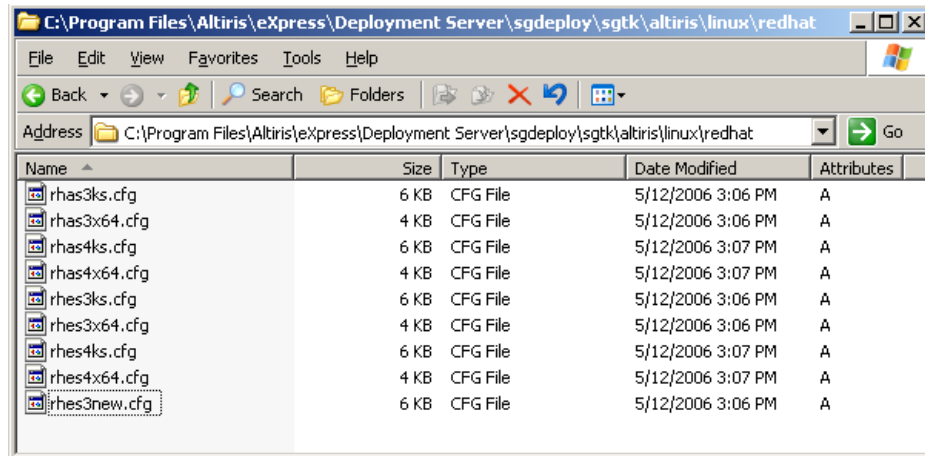


Figure 5-11 Red Hat Linux kickstart files

6. Open in a Linux text editor the rhes3new.cfg file you just created.

Important: The Linux kickstart files cannot be edited or saved using a Windows text editor. They must be edited and saved using a Linux text editor such as WinVi and VIM.

7. Scroll down the kickstart file until you find the following line:

```
url --url http://192.168.0.25/sgdeploy/os/rhes3/
```

First, change the IP address to match the IP address of your Deployment Server. In our test environment the Deployment Server has the IP address 192.168.55.2. Secondly, make sure the path is correctly pointing to the directory where you have copied the Red Hat Enterprise Linux 3 installation media. After we made the changes our line looked like the following:

```
url --url http://192.168.55.2/sgdeploy/os/rhes3/
```

```
#####
# Installation Media Configuration
#
# The following lines should be equivalent to:
# HTTP: url --url http://%SRV_IP%/path/to/OS/files
# NFS:  nfs --server %SRV_IP% --dir /path/to/OS/files
#####

# nfs --server 192.168.0.25 --dir /var/www/sgdeploy/os/rhes3
url --url http://192.168.0.25/sgdeploy/os/rhes3/

#####
# Handle Invalid Partition Tables
#
# 'zerombr yes' indicates that you would like the Red Hat
# installation program to initialize all invalid partition
# tables on disks visible at the time of installation
```

Figure 5-12 The first line in a Linux kickstart file that needs to be changed for your environment

8. Scroll down the kickstart file until you find the following line:

```
mount -t smbfs -o username=sgtk0clnt,password=sgtk0clnt
//192.168.0.25/eXpress /mnt/altiris
```

Again, change the IP address to match the IP address of your deployment server. In addition to the IP address, you need to change the username and password variables to a user with administrative permissions on your deployment server. After we made the changes our line looked like the following:

```
mount -t smbfs -o username=administrator,password=passw0rd
//192.168.55.2/eXpress /mnt/altiris
```

Note: If you enter a password into a kickstart file it will be shown in clear text and readable by any user with the right to access the Deployment Share.

9. When you have finished making changes to the kickstart file, close and save the text file.

5.2.6 Creating a Linux Scripted Install job

When you have copied the operating system installation media to the ServerGuide Scripting Toolkit source tree and created a kickstart file, you can edit the scripted install job tasks to point to the directories housing the installation media and kickstart file. However, before altering the job, make a copy to edit so the original template job is not overwritten.

In the following examples we will alter a scripted install job for Red Hat Enterprise Linux 3. Follow the steps below to create a custom job:

1. Open the Deployment Console.
2. In the Jobs pane, expand to folder IBM ServerGuide Scripting Toolkit - *version (release_date)* → IBM BladeCenter / xSeries / eServer Support → Scripted OS Installation

Inside this folder are a number of other folders that contain the jobs for each version of supported operating systems.

3. Expand the folder labelled **Red Hat Enterprise Linux AS/ES 3**. Expand the folder labelled **Enterprise Linux 32bit**.

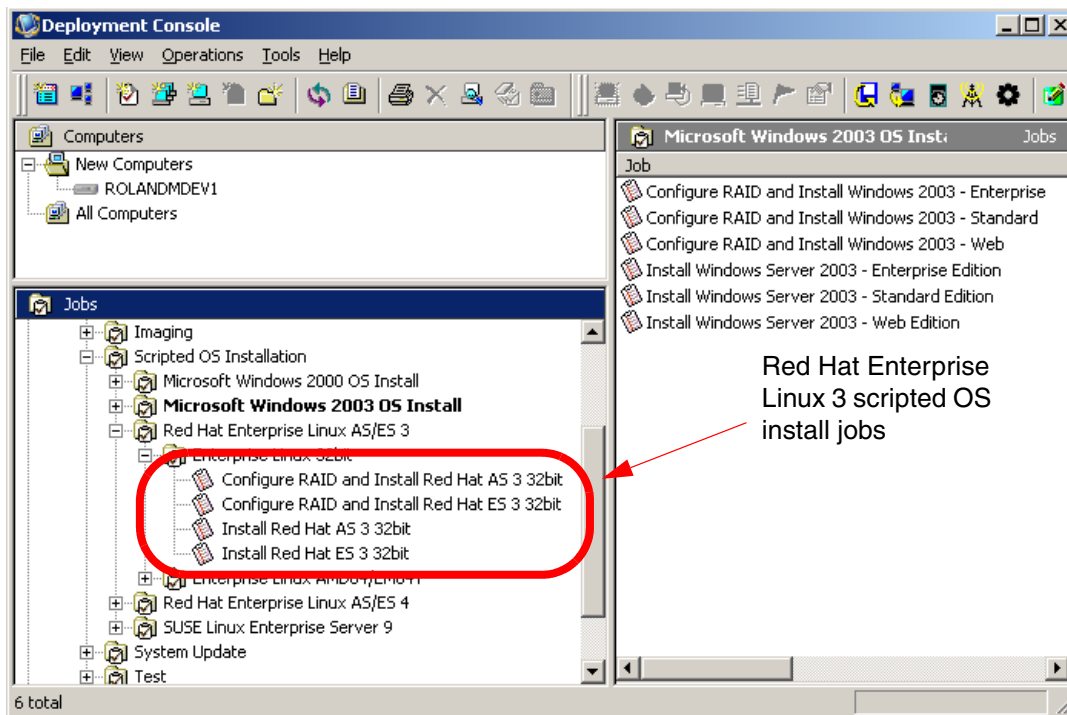


Figure 5-13 Deployment Console with a few of the Red Hat Enterprise Linux 3 scripted install jobs

4. Right-click the job labelled **Install Red Hat ES 3 32bit** and select **Copy** from the pop-up menu.
5. Right-click an area in the Jobs pane and select **Paste** from the pop-up menu. Now you can alter the tasks in this job without overwriting the original job template.
6. Select the job you just copied and in the details pane select the task named **Customize Red Hat Linux Variables**. Now click **Modify** to open the task in edit mode.

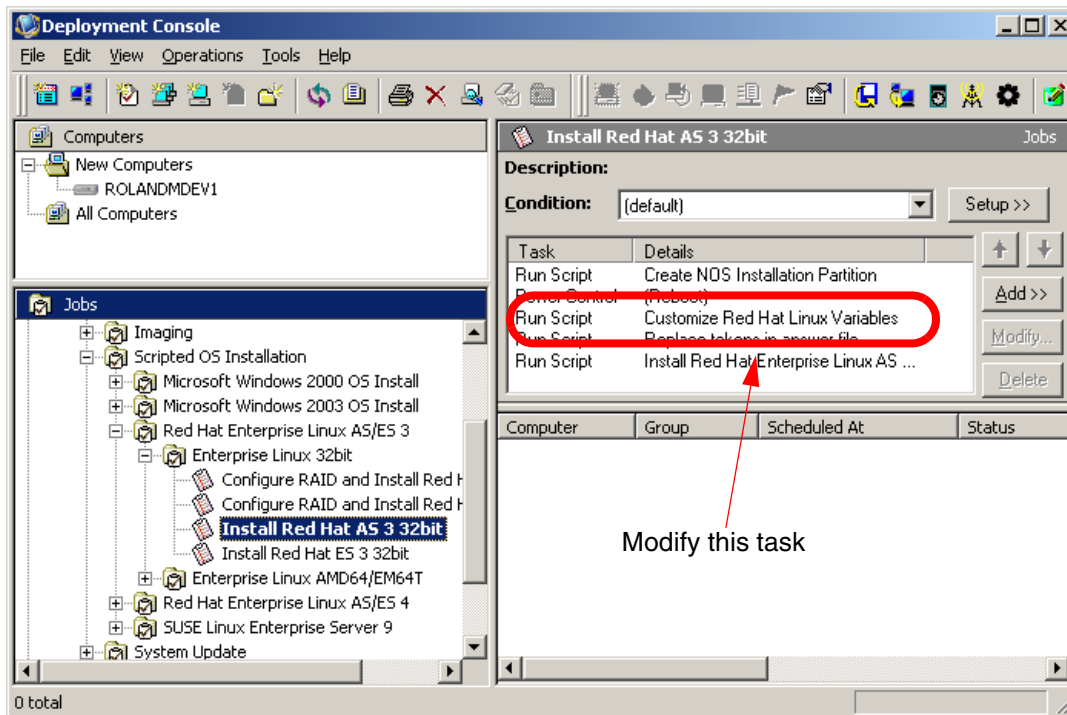


Figure 5-14 Deployment Console with the tasks for a Red Hat Linux scripted OS install job

7. Scroll down the script until you locate the following variable:

```
set SRV_IP=192.168.0.1
```

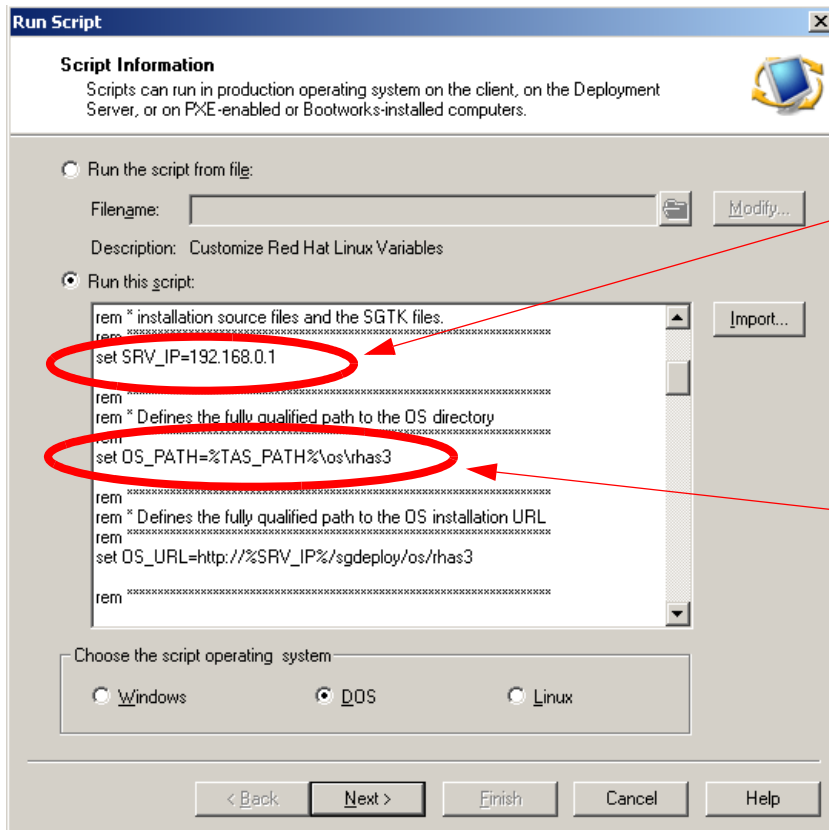
Change the IP address to match the IP address of your deployment server. In our test environment the Deployment Server has the IP address 192.168.55.2. To match our environment we changed the line to the following:

```
set SRV_IP=192.168.55.2
```

8. Scroll down the script until you locate the following variable:

```
set OS_PATH=%TAS_PATH%\os\rhas3
```

Verify that this path is the path to your Red Hat installation media. If it is not correct, change the path to match your environment. In our test environment we copied the Red Hat installation media to the same directory so we did not change this variable.



Change this IP to the IP address of your Deployment Server

Change this path to match your environment

Figure 5-15 The Customize Red Hat Linux Variables task before changes have been made

9. Scroll down the script until you locate the following variable:

```
set ANS_FILE=rhes3ks.cfg
```

Change the path to point to your custom kickstart file. In our case we are using the kickstart file we created above, named rhes3new.cfg. We changed the path to the following:

```
set ANS_FILE=rhes3new.cfg
```

10. After making the required changes, click **Next** to continue.
11. Click **Finish** on the Script Information window to close the task editor.

The custom job for deploying a scripted install of Red Hat Enterprise Linux 3 is complete.

Drag the job you created onto an active computer or group of computers in the Computer pane of the Deployment Console to deploy a scripted install of Red Hat Enterprise Linux 3.

5.3 Deploying VMware ESX Server 2.5

Before deploying a scripted install of VMware ESX Server 2.5 from Altiris Deployment Solution, some setup must be done. The following list summarizes the steps that must be performed before deploying an install of VMware ESX Server 2.5:

- ▶ Copy the installation media to the ServerGuide Scripting Toolkit source tree
- ▶ Configure HTTP and FTP for serving the installation files
- ▶ Customize a kickstart file
- ▶ Customize a deployment job with the script and imaging tasks

This section describes these steps in detail.

5.3.1 Copy the installation media to the Deployment Share

Before creating a customized job to deploy ESX Server 2.5, the installation files need to be copied to the ServerGuide Scripting Toolkit source tree.

Follow the steps below to copy the installation media:

1. Insert the installation media for VMware ESX Server 2.5 into the CD-ROM drive.
2. Using Windows Explorer open the CD and copy the entire contents to directory: `.\sgdeploy\os\ESX25`

Note: By default the ESX25 directory does not exist and will need to be created.

5.3.2 Configuring HTTP and FTP for installing ESX Server 2.5

Linux uses a different method than Microsoft uses for transferring installation files to the Target Computer. Linux requires an FTP server to serve the operating system installation files.

To deploy a scripted install of ESX Server 2.5 you must first install Microsoft IIS on your Deployment Server. This document assumes a working knowledge of Microsoft IIS.

After you have installed IIS, create a new virtual directory. Enter `sgdeploy` as the alias for the virtual directory and point it to the ServerGuide Scripting Toolkit source tree (the `sgdeploy` directory in the Deployment Share). Allow **Read** (default) and **Browse** permissions by checking the appropriate check boxes.

After you have created the virtual directory you need to change the MIME Types of the directory. Follow the steps below to change the MIME Types:

1. Right-click the **sgdeploy** virtual directory and select **Properties** from the pop-up menu.
2. Select the **HTTP Headers** tab.
3. Click **MIME Types** in the MIME Types section.

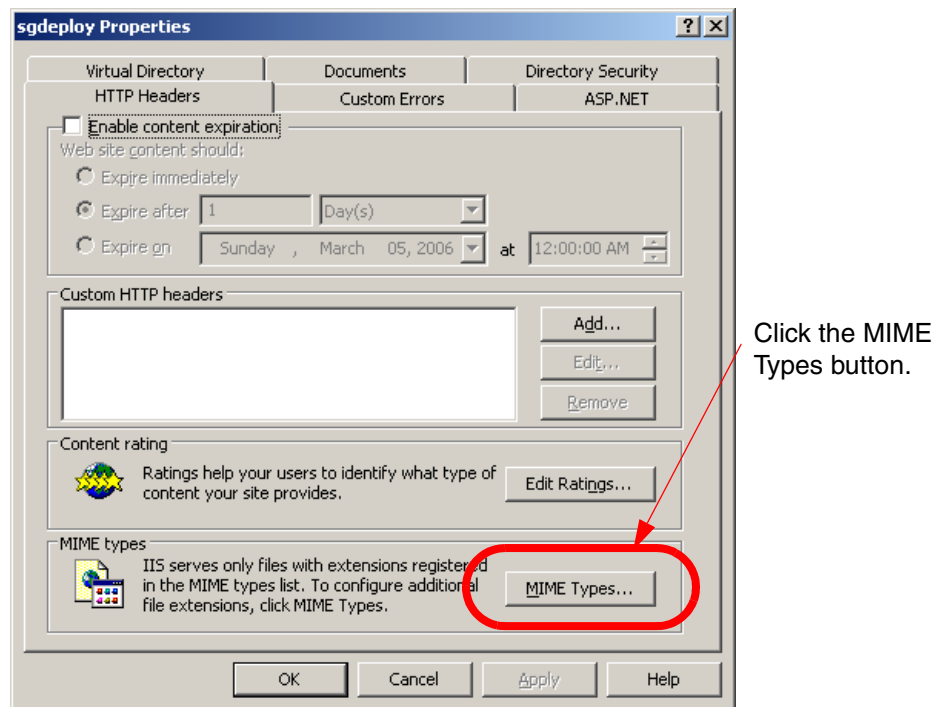


Figure 5-16 The Properties window for the `sgdeploy` virtual directory in Microsoft IIS

4. Click **New**.
5. In the first text box, type `.*` and in the second text box, type `application/octet-stream`.

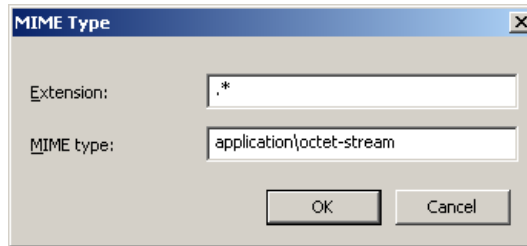


Figure 5-17 The MIME Type window with added text

6. Click **OK**.
7. Click **OK** again to close the Properties window.

The IIS configuration is now complete. When the ESX Server 2.5 install is initiated, the Target Computer(s) will download the installation media from the virtual directory.

Creating a kickstart file

The kickstart file is a standard Red Hat kickstart installation file with some special commands for VMware and ADLagent. For more information about kickstart files refer to Red Hat official documentation at the following URL:

<http://www.redhat.com/docs/manuals/linux/>

The easiest way to create this file is to install ESX Server 2.5 on a computer and then go through the Scripted Install Wizard on the VMware Management Interface under the options tab. That wizard will walk you through the process of getting the information you need and then creating the kickstart file. It will also help setup ESX Server-specific information like the virtual NICs and partitioning information. This will add special commands to the kickstart file for the ESX Server install.

The beginning of the wizard asks for what installation method is desired. Select **NFS**. In the process of following the wizard, select static IP information for your install. This will setup the file so you can replace the specific IP information with tokens. Figure 5-18 on page 160 shows a portion of the kickstart file after the specific IP information has been replaced by tokens.

```
# Network install type
network --bootproto static --ip=%NIC1IPADDR%
--netmask=%NIC1IPNETMASK% --gateway=%NIC1IPGATEWAY%
--nameserver=%NIC1IPDNS1% --hostname=%NIC1IPHOST%
```

Figure 5-18 A portion of the kickstart file showing information that has been replaced with tokens

The previous example is some of the information that is replaced when the job is preprocessed before executing the job. The sample job labeled *Scripted Install of ESX points to a sample kickstart file (ks.cfg) that can be used as a reference. This file should be modified or replaced with the file being used.

When selecting a computer to run the ESX Server 2.5 install on, make sure the information that is to be replaced is in that computer's record or you could have a problem with the token replacement. For instance, if the computer is setup for DHCP and there is no specific IP information for IP address or netmask, etc, the tokens will be set to blank when replaced.

Figure 5-19 is a list of some of the other VMware specific kickstart commands (notice that vmswap is also tokenized).

```
# VMware-specific kickstart commands
vmaccepteula

#PCI Device Allocation and COS memory
vmservconmem --reserved=192
vmpcidivv --auto

#VMware License information
vmserialnum --esx=<YOURSERIALHERE> --esxsmp=<YOURSERIALHERE>

#VMware Network config
vmnetswitch --name="Vir1" --vmnic=vmnic0
vmnetswitch --name="Vir153k37"

#VMware Swap config
vmswap --volume="vmfs" --size=1000 --name="%NIC1IPADDR%-0.vswp"
```

Figure 5-19 Another portion of the kickstart file showing information that has been replaced with tokens

For further information about the Scripted Install wizard see the VMware ESX Server documentation available from:

<http://www.vmware.com/support/pubs/>

You will notice at the bottom of the kickstart file there is a %package command for the ESX Server install and a %post command. The post command installs ADLagent in three steps:

1. The adlagent.custom.config file is copied to the directory where ADLagent is run. This file tells ADLagent how to connect to the server.
2. The ADLagent RPM that installs ADLagent is run.
3. The configuration of the ADLagent service is run.

In the future, ADLagent will be installed using a BIN file instead of RPM. In this case you will not need to do the final configuration step.

The kickstart file with the embedded tokens is now used in a token-replacement job in Deployment Solution. The job creates new custom kickstart files which are then used on each of the target servers to install ESX Server.

Note: Another potential problem with the kickstart file is extra control characters that are put in by some Windows text editors. If you edit the kickstart file using Notepad there will be Carriage Return characters at the end of the lines that the kickstart processor will not handle properly. To fix this run the following command in Linux on the file to remove the CR characters.

```
tr -d "\r" < ks.cfg > ks2.cfg
```

Alternatively, you can use a Linux-based text editor such as VIM or WinVI to edit the kickstart file.

The ADLagent install files need to be available during the install process. Another NFS mount point can be used for the ADLagent install files. Copy in the ADLagent RPM file and the custom.config file.

5.3.3 Customize a deployment job with the script and imaging tasks

Altiris Deployment Solution has a sample template job for deploying ESX Server. The ***Scripted install of ESX** job can be found in the ESX Scripted Install folder. To find the job, open the Deployment Console and in the Jobs pane, browse to folder:

Samples → VMware → Scripted Install → ESX Scripted Install

The *Scripted install of ESX job is shown in Figure 5-20 on page 162.

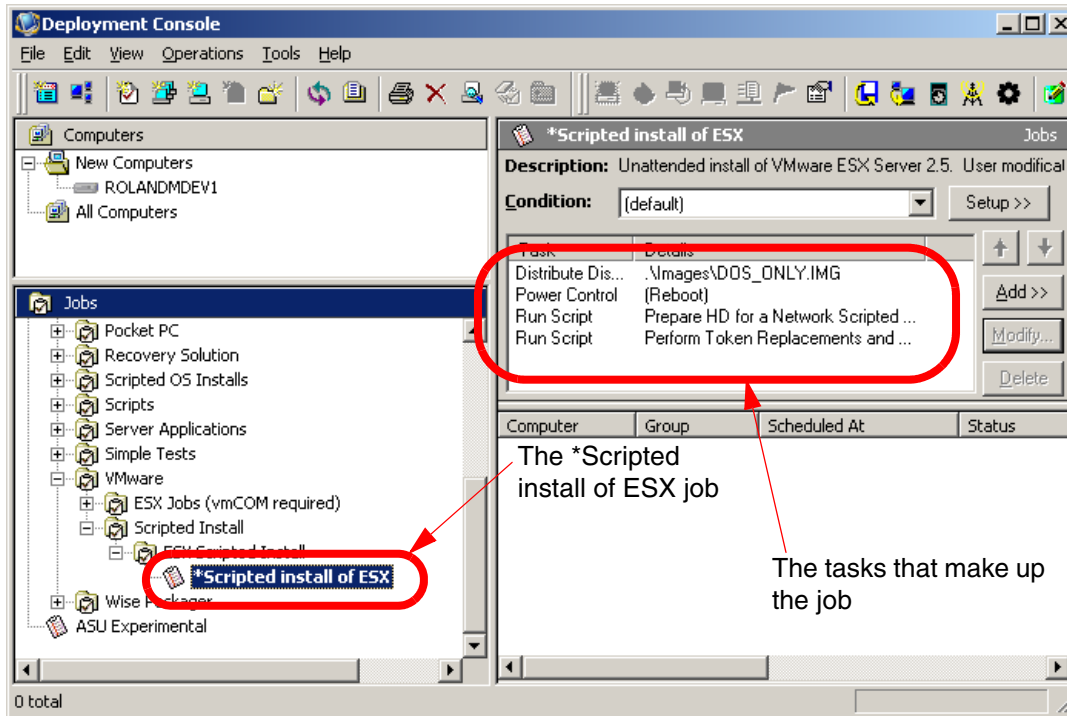


Figure 5-20 The Deployment Console with the *Scripted Install of ESX job

The *Scripted install of ESX job contains four tasks:

1. The first task, labelled Distribute a DOS image, uses the DOS_ONLY.IMG to create a temporary 2 GB partition on the Target Computer's hard disk drive. This is where the kickstart and startup files will be copied to for performing the installation. The partition is removed after installation completes.

Important: Open the task in edit mode by selecting the task in the Details pane of the Deployment Console and clicking **Modify**. Make sure the check box labelled **Automatically perform configuration task after completing this imaging task** is unchecked. The configuration for the box is taken from the initial deployment configuration or new computer at token replacement time. Therefore a post image configuration is not necessary.

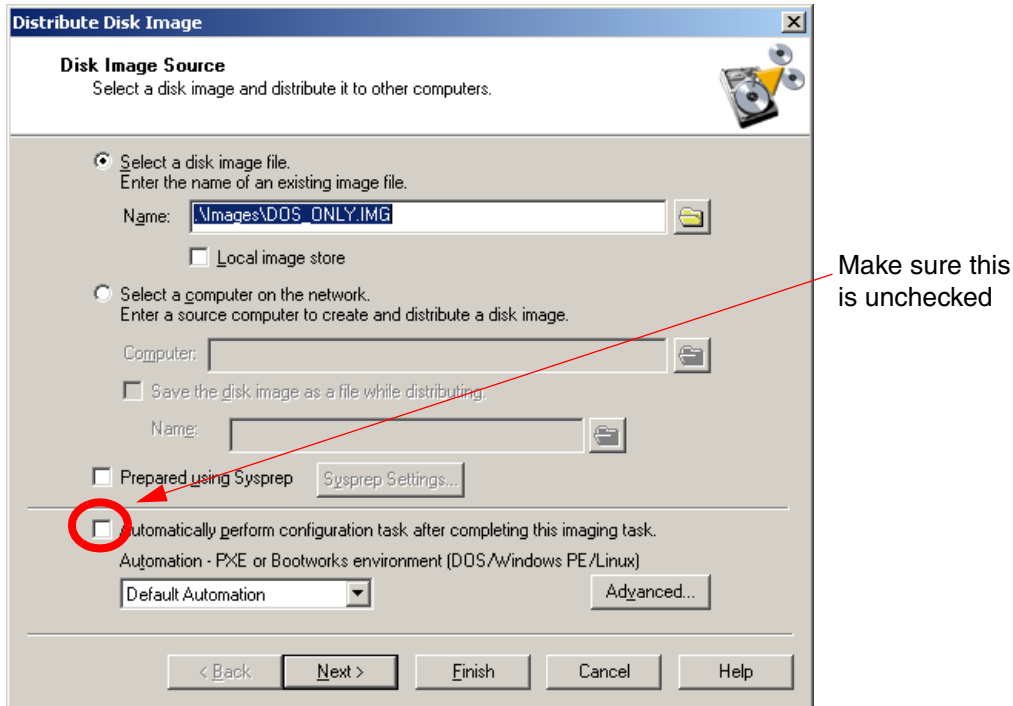
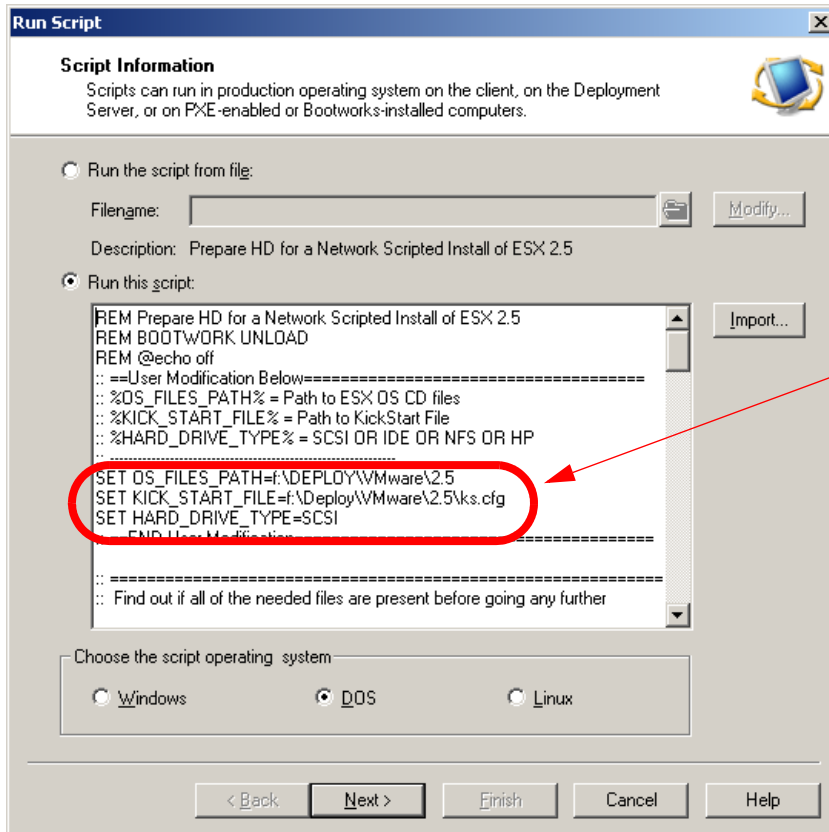


Figure 5-21 The Distribute DOS image task

2. The second task, labelled (reboot), is a simple restart task. It assures the computer is done with the image task and there is nothing in memory.
3. The third task, labelled **Prepare HD for a Network Scripted Install of ESX 2.5**, is a script task that copies the necessary files to the Target Computer so a kickstart installation can be done and then creates an autoexec.bat file.

The script first creates environment variables used in copying files and creating the proper autoexec. Variable %OS_FILES_PATH%, is the path to the kickstart execution files and %KICK_START_FILE% is the path to the kickstart file itself.

The kickstart execution files are: loadlin.exe, vmlinuz, initrd.img. The kickstart file is named ks.cfg. All of these files are from the ESX Server 2.5 install CD except ks.cfg. Loadlin.exe is in the \dosutils directory and vmlinuz and initrd.img are in the \images\pxeboot directory.



These variables can be customized to match your environment

Figure 5-22 The Prepare HD for a Network Scripted Install of ESX 2.5 job

These files should be copied to a location where the deployment server can access them when running the job. In the sample job, the directory is off the deployment share in the `deploy\VMware\2.5` directory. By default, this directory does not exist. Open the deployment share and inside the `deploy` directory create a new folder and name it `vmware` and inside that directory create a new folder and name it `2.5`.

The third environment variable, `%HARD_DRIVE_TYPE%`, is the type of hard drive on the Target Computer. This is necessary so the right command will be sent to start the installation and find the kickstart file. The types are SCSI, IDE, NFS and HP.

Note: SCSI looks for the kickstart file on `sda1`.

The script then checks for the files used to start the kickstart installation and copies them to the local hard drive except for the kickstart file. The kickstart file is copied to a location on the server where it can be found and token replaced in the next task.

The script then creates the appropriate autoexec.bat based on the hard drive type and exits.

4. The fourth and final task, labelled **Perform Token Replacements and Launch Scripted Install**, is fairly simple but does quite a lot. There are several REM lines (REM lines are remarks and will not affect the running of the script) at the beginning of the script that help set up for the autoexec.bat execution as shown in Figure 5-23 on page 166.
 - The first unloads bootworks so there is sufficient memory for the install.
 - The second is the command that does the token replacement on the kickstart file. This replaces the tokens in the kickstart with the configuration information from the computer being installed.
 - The third lets the server know that the machine is going to reboot and to make the task successful no matter what happens to the client.

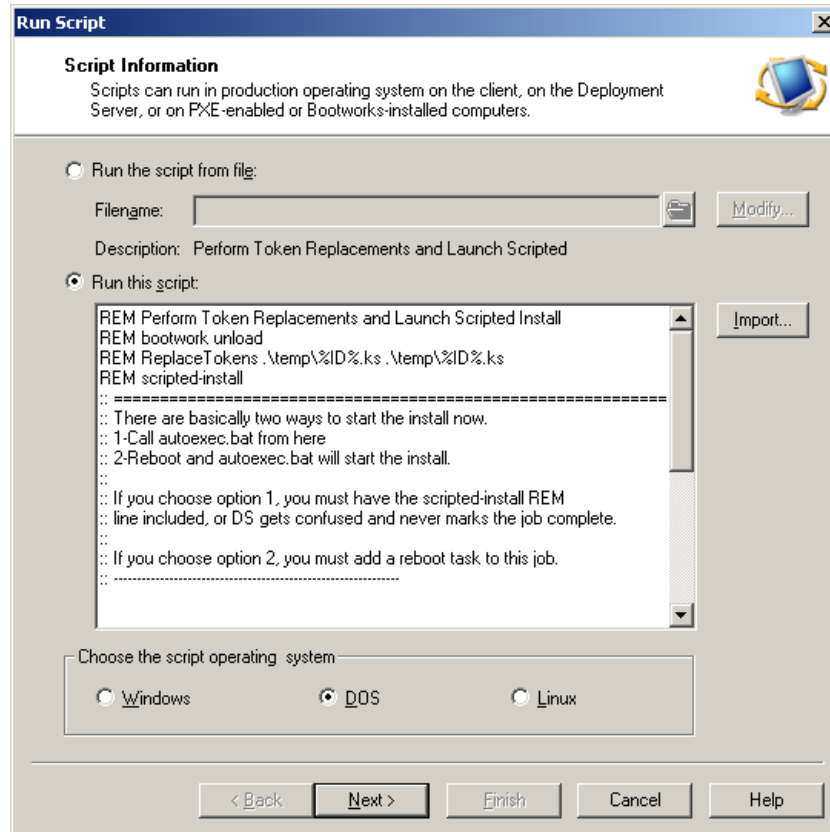


Figure 5-23 Script "Perform Token Replacements and Launch Scripted Install"

Now that the server has done the token replacement on the kickstart file, it can be copied to the client machine. After this is done the autoexec.bat is called and that starts the installation.

After you have configured the tasks to match your environment click **Finish**.

Your custom ESX Server 2.5 installation job is ready for deployment. You can deploy it by drag-and-dropping the job onto any active computer or group of computers in the Computers pane of the Deployment Console.



Using image-based deployment

Image-based deployment, also referred to as *cloning* or *imaging*, is a method of deployment that captures the exact state of a computer's hard drive and saves the information in an image file. The image file is saved on a file server (or network share), and is later duplicated onto other computers creating exact replicas of the original system. The disk image contains the partition information, the boot sectors, the file allocation table, and the operating system including application software and settings.

This chapter covers the basics of image capture and deployment using Altiris Deployment Solution. Images are created and deployed using the RapiDeploy utility (`rdeploy.exe`), that is bundled with Altiris Deployment Solution.

The following topics are discussed:

- ▶ 6.1, “Comparing with Symantec Ghost Solutions Suite” on page 168
- ▶ 6.2, “Image-based deployment versus Script-based deployment” on page 169
- ▶ 6.3, “Imaging Windows and Linux” on page 170
- ▶ 6.4, “Integrating Sysprep with Deployment Solution” on page 193
- ▶ 6.5, “Creating hardware independent Windows images” on page 202
- ▶ 6.6, “Imaging with Windows PE” on page 220

6.1 Comparing with Symantec Ghost Solutions Suite

Altiris Deployment Solution and Symantec Ghost Solutions Suite are both industry leading imaging applications. Both applications include very powerful base tools to ease management of large environments. However, we believe the advanced features in Altiris Deployment Solution sets it apart from the Symantec offering.

6.1.1 Common features

Altiris Deployment Solution 6.5 and Symantec Ghost Solutions Suite have many basic features in common:

- ▶ An agent that can be installed on client computers for greater manageability
- ▶ Support for both boot media (CD or diskette) and network boot by integrated PXE server software
- ▶ An integrated utility to change the Security Identifier (SID) of target computers
- ▶ A graphical management console
- ▶ Integrated support for Sysprep
- ▶ Both products can change the configuration of target computers such as host name, network settings, and workgroup/domain membership
- ▶ Both products support resizing of the partitions on target computers
- ▶ A client migration tool

6.1.2 Altiris Deployment Solution

While both applications include the basic tools for disk imaging, Altiris Deployment Solution's advanced features differentiate it from Symantec Ghost Solutions Suite. The following is a list of Altiris Deployment Solution's advanced features:

- ▶ Can manage IBM BladeCenter servers at the rack level
- ▶ Integrates with the IBM Scripting Toolkit for increased manageability of IBM System x Servers. See 2.2, "Integrating the ServerGuide Scripting Toolkit" on page 28.
- ▶ A simple install with integrated tools
- ▶ Altiris Deployment Solution includes a tool to remotely install the Altiris Client (AClient) on target computers through the Deployment Console. The AClient enables:
 - The ability to backup the Windows Registry

- A basic remote control (similar to Remote Desktop)
- Power control (wake-up, restart, shutdown, log off)
- ▶ An Initial Deployment feature to install and provision bare-metal computers the first time they contact the Deployment Server, either through PXE or boot media
- ▶ A Boot Disk Creator tool to create boot disk images that include various boot environments such as DOS (Windows 98 or FREE DOS), Linux, or Windows PE
- ▶ Support for scripted operating system installation (both Windows and Linux)
- ▶ An Image Explorer tool to edit, delete, or add files on an existing image
- ▶ Can manage multiple Deployment Servers

6.1.3 Symantec Ghost Solutions Suite

Although not as feature rich as Altiris Deployment Solution, Symantec Ghost Solutions Suite includes some features lacking in Altiris Deployment Solution:

- ▶ Integrated support for USB and FireWire storage devices
- ▶ Can write images directly to a CD or DVD
- ▶ Can create incremental images (primarily used as a backup solution)

6.2 Image-based deployment versus Script-based deployment

Script-based deployment is simply an automated unattended operating system install. For Windows, a scripted installation copies the i386 folder and drivers to the target computer and runs the Windows install locally. Image-based deployment is creating an image of a computer's hard drive and copying that image onto other machines, creating clones of the original.

There are many reasons to choose image-based deployment rather than script-based deployment for your deployment strategy. The following list highlights some of the key benefits:

- ▶ Image deployment has much faster deployment times (typically less than 10 minutes for image based instead of 40 minutes for script-based installs).
- ▶ Images can be multicasted across the network. RapiDeploy supports both unicast and multicast methods of deployment. This is covered in more depth in 6.3.3, "Using multicast" on page 182.

- ▶ If the image is made self-extracting, it can be deployed via CD, DVD, network drive, etc. without requiring the need to have a Deployment Server in place.

Self-extracting images will not be covered in this redbook, but if you want to learn more, refer to *Altiris Deployment Solution 6.5 Reference Guide*. The guide can be found at the following URL:

http://www.altiris.com/upload/deployment_002.pdf

The downfalls to image-based deployment are:

- ▶ The image is outdated the moment it is created. This makes it difficult to maintain software version control. Any new service packs, hot fixes, drivers, etc. that are released after the initial image creation must be reflected if having a current image is important to you.
- ▶ Image management can be quite burdensome. Maintaining an image for each System x machine type can be very time consuming if your site has many different models. However, it is possible to create a hardware-independent image, reducing the need for multiple images. To learn more about creating hardware independent images see 6.5, “Creating hardware independent Windows images” on page 202.

6.3 Imaging Windows and Linux

Altiris Deployment Solution supports imaging on both Windows and Linux. This section covers imaging for both Windows and Linux.

Performing an image capture and image deploy with Linux is the same as with Windows with a few exceptions.

- ▶ In the current release, Altiris Deployment Solution supports only the ext2 and ext3 Linux file systems. If you are using a different file system, Altiris Deployment Solution will fail to capture or deploy an image.
- ▶ If software RAID is being used on the target computer image capture and image deployment will fail.

6.3.1 Capturing a donor image

Before image deployment can begin, a computer must be prepared to donate an image for later deployment. This computer is called the *Reference Computer*.

Preparing the Reference Computer for image capture (Windows only)

The following steps list basic instructions for setting up a Reference Computer. These instructions assume you will be installing a Windows Server operating system with the intent to capture its image for mass distribution to System x computers of the same model type. For different models, see 6.5, “Creating hardware independent Windows images” on page 202.

1. Install the Windows Server operating system using the IBM ServerGuide CD that shipped with your computer or with the Windows Server installation media.

Using the ServerGuide CD is easy to use and very straight forward. All you have to do is boot from the ServerGuide CD and follow the prompts. Make sure you have a copy of your Windows Server media and product key handy. Consult your IBM Server documentation if you need specific instructions on how to use the ServerGuide CD.

2. Install any service packs, hotfixes, software, and so forth on the Reference Computer.

Keep in mind, the more software you install to your Reference Computer, the larger the donor image is going to be and the longer it is going to take to deploy. Some best practices are to repackage the applications you want to deploy and deploy them after the image has been installed via Deployment Solution and the agent (AClient) that resides on the computer. This allows you to provide better software version control and allows you to keep your image longer without having to constantly update it when newer software becomes available.

3. Alter any operating system or application settings that you want to have replicated throughout your environment. Operating system settings might include power options, desktop settings, screen saver options, and so forth.
4. Install the Deployment Agent (AClient). See 2.3, “Installation and integration of the Deployment Agent” on page 46.
5. Run Microsoft Sysprep on the Reference Computer to replace the SID and rebuild the driver database. When Sysprep has finished it will shutdown the computer. Do not power on the computer until you are ready to connect to the Deployment Server.

For Windows XP and Windows Server 2003, Sysprep is located in the DEPLOY.CAB file located at \SUPPORT\TOOLS on the installation CD. For complete details on how to use Sysprep and how it works, as well as downloading the latest version, go to <http://microsoft.com> and search for **sysprep**.

Note: Altiris Deployment Solution has the ability to integrate with Microsoft Sysprep. Using Sysprep in this manner allows for much more consistent image management. If Microsoft Sysprep has been integrated, simply drag the capture image job onto the Reference Computer to initiate the image capture job. More information about Microsoft Sysprep integration be found in 6.4, “Integrating Sysprep with Deployment Solution” on page 193.

Important: Do not let the Reference Computer boot into the operating system as this will initiate the Sysprep process before the image is captured. If the Reference Computer does boot to the operating system before the image is captures, repeat Step 5.

Connecting to the Deployment Server

Before capturing an image, the Reference Computer needs to be connected to the Deployment Server. If you plan use PXE, verify the following before powering on your Reference Computer:

- ▶ The Altiris PXE Server that is bundled with the installation has been installed and the PXE services are running.
- ▶ Your Reference Computer has PXE enabled in the BIOS and is configured to boot from the network.
- ▶ Your Reference Computer is physically connected to the network.
- ▶ Your DHCP server is active (with a scope defined) and on the same network as your Reference Computer.

Note: Connecting to the Deployment Server using PXE is covered in greater detail in 2.5, “Configuring and using PXE pre-boot environment” on page 64.

After you have verified the configuration you are ready to connect to the Deployment Server. Power on your Reference Computer and select the PXE boot image of your choice from the PXE boot menu to connect to the Deployment Server.

When connected, the Altiris PXE Server will download a boot image to your Reference Computer. When your Reference Computer displays the following message you are ready to initiate the image capture process:

The deployment server has instructed Bootworks to wait.

Initiating the image capture process

Image capture is initiated from the Deployment Console rather than the Reference Computer.

Follow the steps outlined below to capture the donor image:

1. Open the Deployment Console. You should see a computer icon with a yellow yield sign located under the New Computers group in the Computers pane. This icon represents a system that has contacted the Deployment Server and is not recognized by Deployment Database.

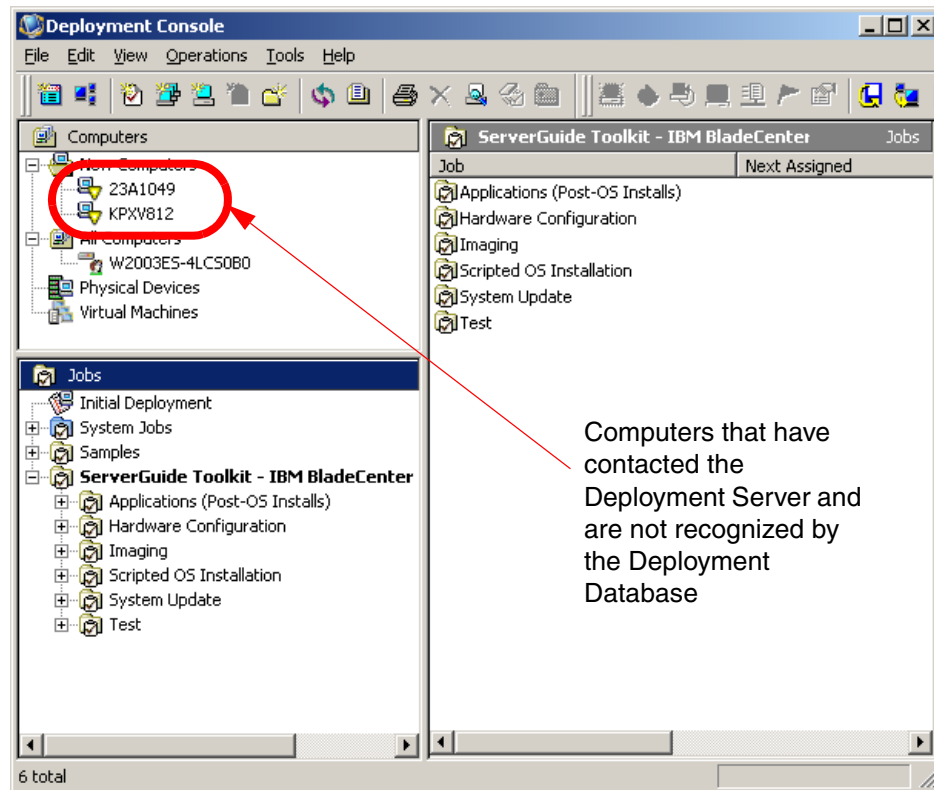


Figure 6-1 Altiris Deployment Solution Console with system waiting for job assignment

2. Create a new job by clicking **File** → **New** → **Job Wizard**. The Job Wizard appears. Select **Create an Image** and type a name for the job. Click **Next**.

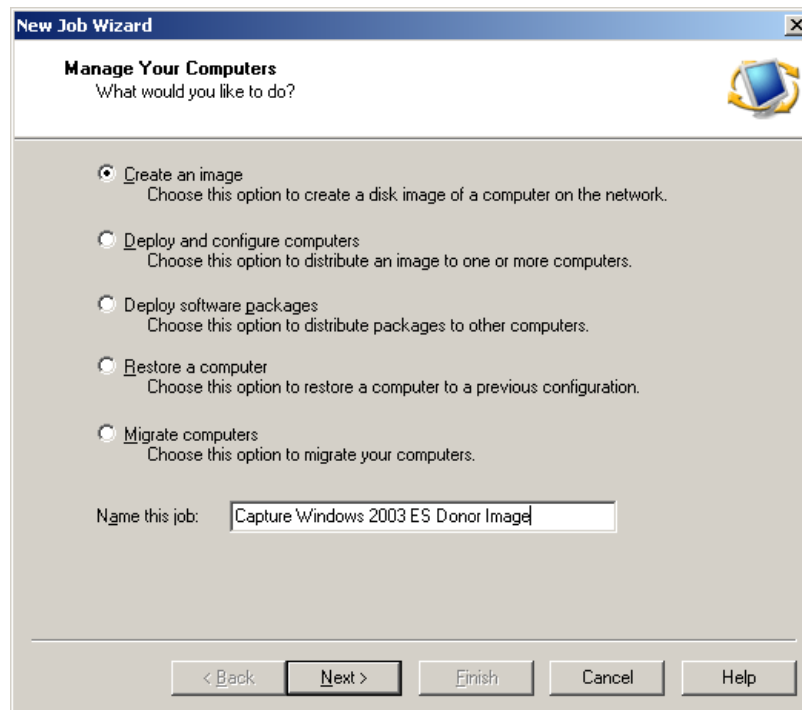


Figure 6-2 New Job Wizard

3. Select the computer you want to use as your Reference Computer in the Select Computer window. Click **Next**.
4. On the Save Disk Image to a File window click the **Folder** icon and navigate to the Images folder, located in the eXpress share. Save the file using the **.img** extension and surround the filename with quotation marks to ensure it is saved with the correct extension. For example: "Windows2003.img".

Note: Saving an image with the **.exe** extension creates a self-extracting image that can be deployed using CD or DVD media, without the need of a Deployment Server. Self-extracting images will not be covered in this redbook, but if you want to learn more, refer to *Altiris Deployment Solution 6.5 Reference Guide*.

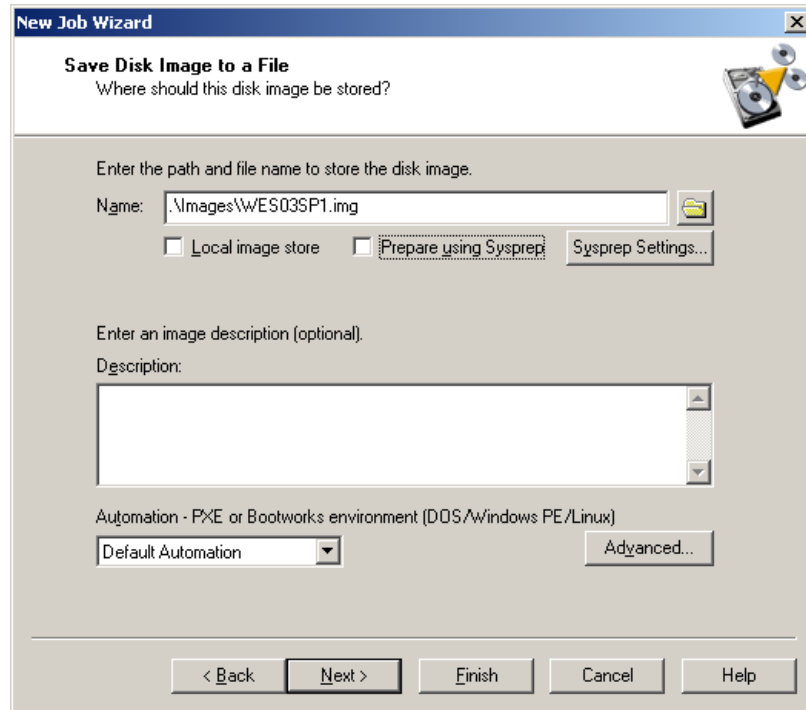


Figure 6-3 Save Disk Image to File window

Note: If you want to use the integrated Sysprep functionality you would check the check box labeled **Prepare using Sysprep** and alter the settings by clicking **Sysprep Settings** (Windows only). For more information about integrating Sysprep, see 6.4, “Integrating Sysprep with Deployment Solution” on page 193.

5. If you are imaging a Linux operating system, click **Advanced**. In the Create Disk Image Advanced window make sure the check box labeled **Do not boot to Windows** is checked. Click **OK** to close the Create Disk Image Advanced dialog box. Click **Next**.

Note: If you use Sysprep without integrating it with Altiris Deployment Solution this will ensure the Reference Computer does not boot into Windows initiating the Sysprep process before the image is captured.

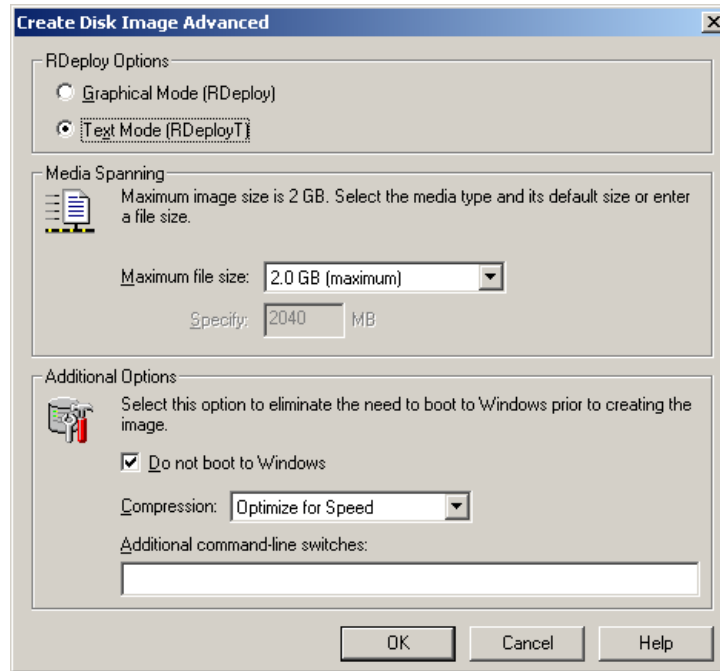


Figure 6-4 Create Disk Image Advanced window with the Do not boot to Windows checked

6. In the Schedule Job window select **Run this job immediately** if you want to execute the job right away. If you would rather save the job for later execution, select **Do not schedule**. Click **OK**.
7. If you selected **Run this job immediately**, your image capture process will start on the Reference Computer. When the image capture job completes, the image will be available for deployment.

6.3.2 Deploying the image

Now that you have created an image it can be deployed to your computers.

Creating a deployment job

Before the image can be deployed you must create a job in the Deployment Console.

Follow these steps to create the deployment job:

1. Open the Deployment Console.

2. Start the Job Wizard by clicking **File** → **New** → **Job Wizard**.
3. When the Job Wizard starts, verify that **Deploy and configure computers** has been selected. Give the job a meaningful name and click **Next**.

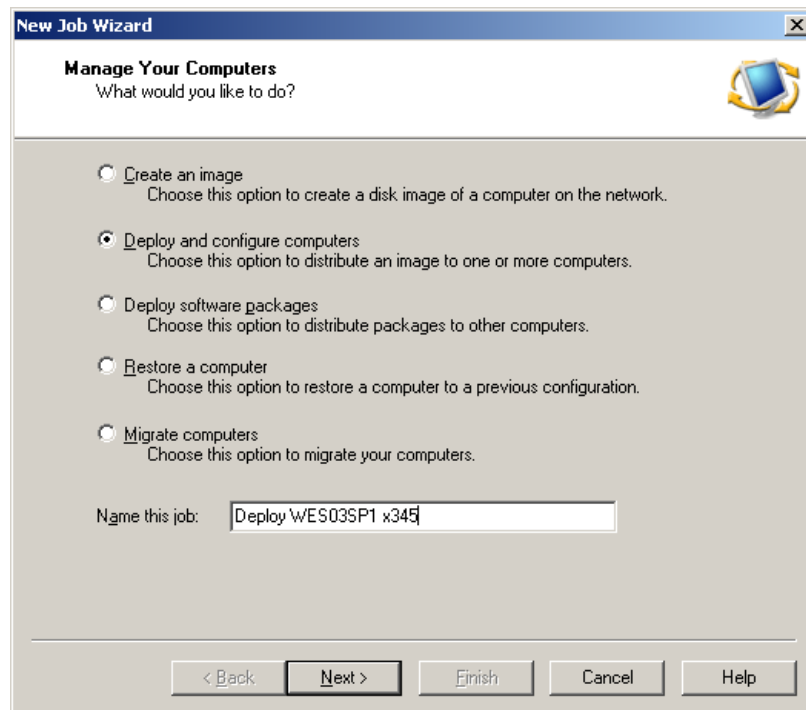


Figure 6-5 Job Wizard with a deployment job selected

4. Click **Next** to bypass the Job Conditions window because we do not use conditions for this job.
5. On the Disk Image Source window, click the Folder button and browse to the image file which you want to deploy. Select the image file and click **OK** to return to the Disk Image Source window. Since we are using Sysprep to configure our image, rather than the Altiris default tool, uncheck the check box labeled **Automatically perform configuration task after completing this imaging task**. Click **Advanced** toward the bottom of the window.

Note: Always uncheck **Automatically perform configuration task after completing this imaging task** if you are deploying a Linux image.

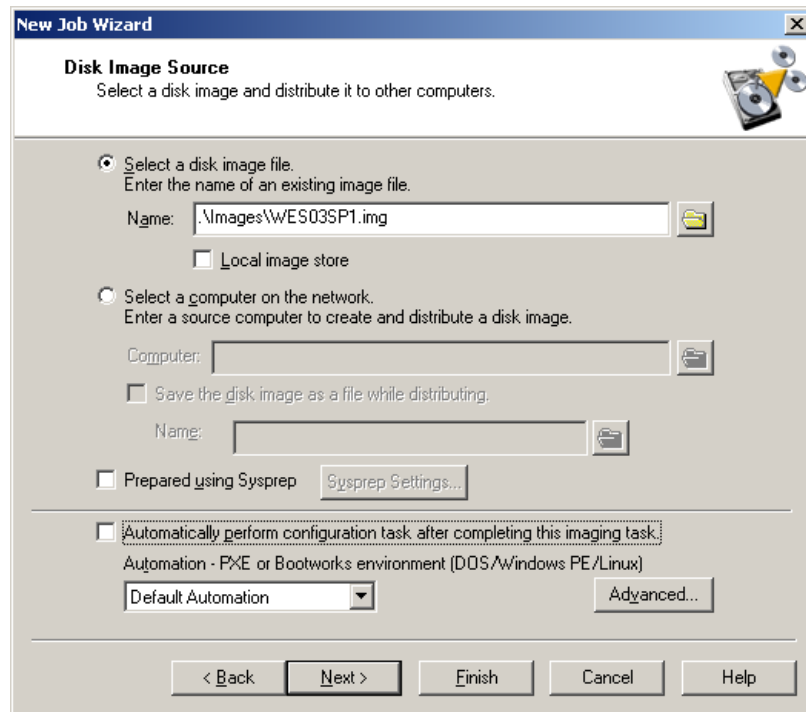


Figure 6-6 Disk Image Source window

Note: If you are using the integrated Sysprep functionality, select **Prepared using Sysprep** and alter the settings by clicking **Sysprep Settings** (Windows only). For more information see 6.4, “Integrating Sysprep with Deployment Solution” on page 193.

6. In the Distribute Disk Image Advanced window you can change the way the image sits on the target computer’s disk.

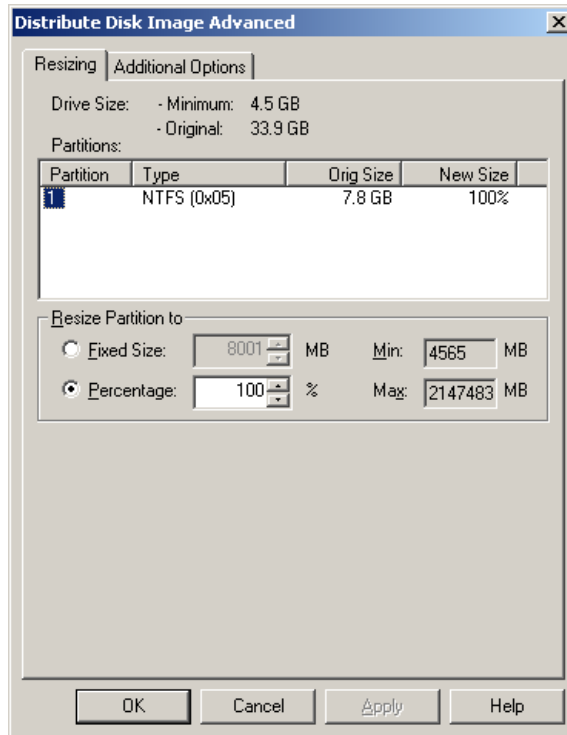


Figure 6-7 *Distribute Disk Image Advanced window Resizing tab*

The Partitions section displays the number of partitions, the type of file system, the original size of the image, and the proposed size on the target computer's disk. You can change the proposed size by selecting either Fixed Size or Percentage and changing the defaults to something more appropriate to your environment. Click on the **Additional Options** tab.

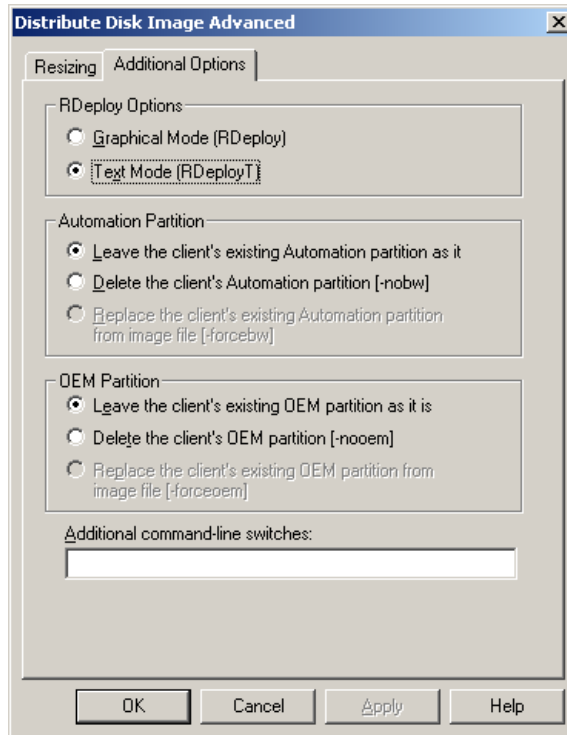


Figure 6-8 Distribute Disk Image Advanced window Additional Options tab

The Additional Options tab has a few noteworthy controls. The RDeploy section controls the graphical view of RapiDeploy. We have found that Text Mode is more stable than Graphical Mode. The Additional command-line switches text box towards the bottom allows you to send switches to the RDeploy.exe application. To see a list of available switches refer to the *Altiris RapiDeploy 6.1 Product Guide*. This guide can be found at the following URL:

<http://www.altiris.com/upload/rapideploypguide.pdf>

We will keep the defaults so click **OK** to return to the Disk Image Source window. Click **Next** to continue.

7. Click **Next** to bypass the RapidInstall and PC Transplant Packages window. We do not want to install any packages at this point.
8. On the Select Computers window, select **Do not apply this job to any computers at this time** to save the job for later deployment. Click **Next**.
9. Click **Finish** to close the Summary window and return to the Deployment Console.
10. Your job will now appear in the Jobs pane of the Deployment Console.

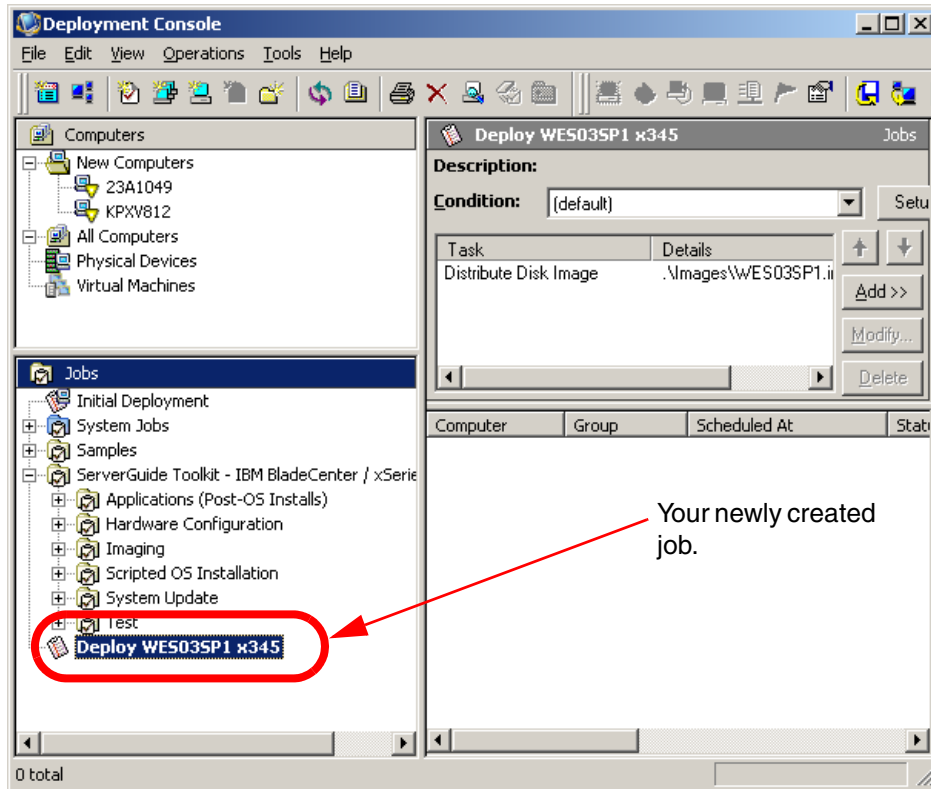


Figure 6-9 Deployment Console with a newly created deployment job

Initiating the deployment job

After you have created the image deployment job you can initiate deployment by dragging the job onto any available computer or computers in the Computers pane of the Deployment Console. Alternatively, you can drag and drop the computer or group of computers onto the job.

If the computer you want to image is not shown in the Computers pane of the Deployment Console you must connect the target computer to the Deployment Server as described in “Connecting to the Deployment Server” on page 172.

When the computer you want to image is available in the Computers pane of the Deployment Console, simply drag the newly created image deployment job onto the waiting computer. When the Schedule Job window appears select **Run this job immediately** and then click **OK**.

6.3.3 Using multicast

RapiDeploy supports two methods of distributing images: unicast and multicast.

With unicast, a copy of the data is transmitted to each target computer. By default, RapiDeploy uses unicast.

With multicast, the image is transmitted once from the Deployment Server to one of the target computers which is selected by the Deployment Server to act as a multicast session manager (called the *Master Computer*). The Master Computer then re-transmits the data to the remaining target computers. The Master Computer is chosen by the Deployment Server through an election process that evaluates the target computers network adapter's MAC address to determine which computer has the newest adapter.

Important: The default PXE boot image (if you installed the MS-DOS files when you installed Altiris Deployment Solution), **DOS Managed**, uses the Intel UNDI driver to communicate with target computers. However, the Intel UNDI driver does not support multicasting.

To enable multicasting, a custom PXE boot image must be created using network adapter drivers appropriate to your environment. Alternatively the default PXE boot image, **DOS Managed**, can be altered to use a network adapter driver suitable for your environment that supports multicasting. Use the PXE Configuration Tool to alter the existing PXE boot images or to create custom images as described in “Enabling multicast” on page 183.

Some points to remember about multicasting:

- ▶ The multicast transmission will only go as fast as the slowest computer in the group.
- ▶ If a single computer fails, it will drop out of the session and the session will continue.
- ▶ You can usually multicast only to computers on the same network subnet because most routers and switches do not allow multicasting. To image computers on another subnet, start a Master Computer on that subnet and connect the target computers to the Master Computer.

Tip: It is a best practice to use multicasting when imaging more than four computers at the same time. This will greatly reduce the load on the network infrastructure.

Enabling multicast

Multicasting is enabled by default; however, as mentioned earlier the default DOS Managed PXE boot image supports only unicasting. If you have not changed the DOS Managed boot image to use the actual network adapter device drivers, unicast will be the method used.

Follow the steps below to configure the default DOS Managed PXE boot image:

1. Open the Deployment Console.
2. Click **Tools** → **PXE Configuration**. This opens the PXE Configuration utility shown in Figure 6-10.

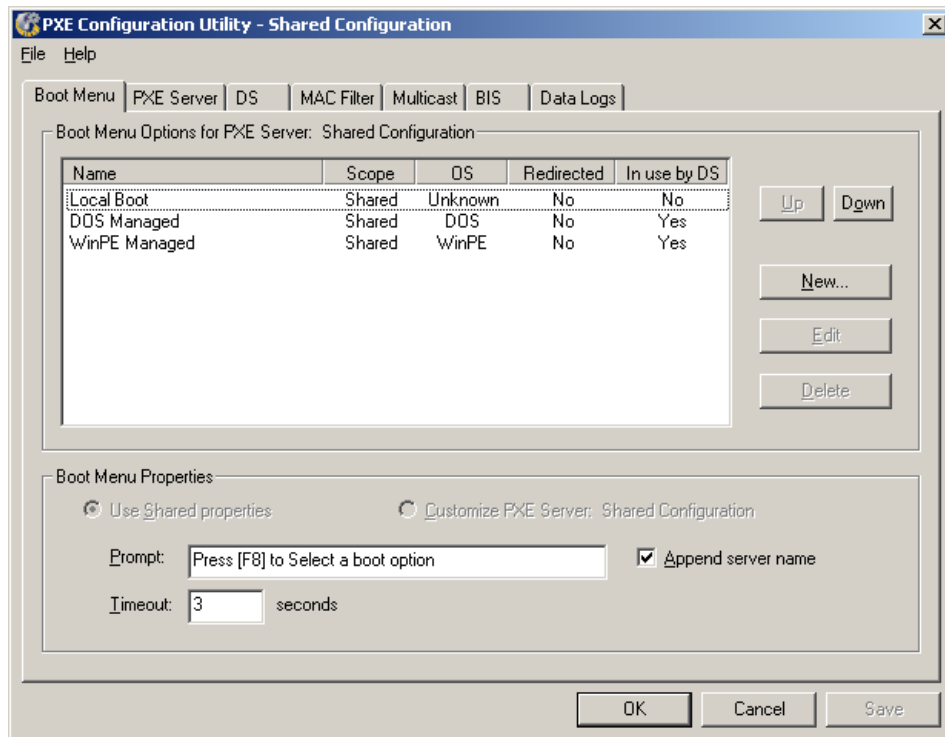


Figure 6-10 The PXE Configuration utility's main window

3. Select **DOS Managed** in the Boot Menu Options for PXE Server section. Click **Edit** to open the Edit Shared Menu Option window for the DOS Managed boot image.

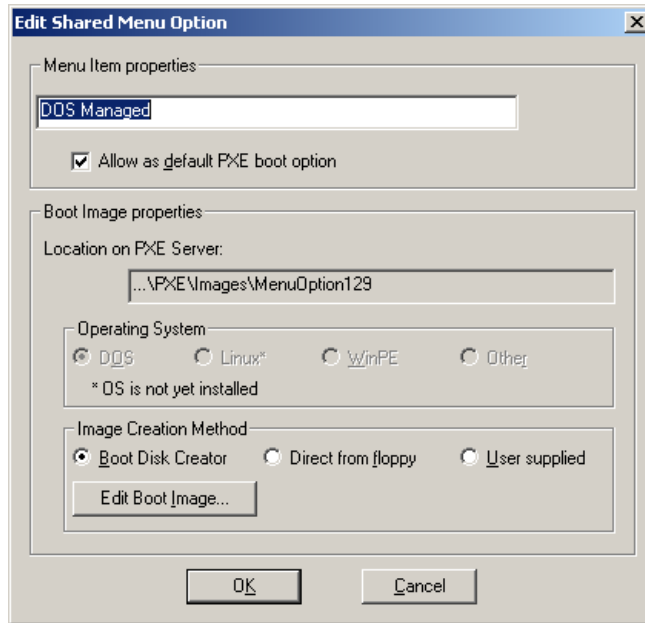


Figure 6-11 The Edit Shared Menu Option window for the DOS Managed PXE boot image

4. Click **Edit Boot Image** to open the Boot Disc Creator tool shown in Figure 6-12 on page 185.

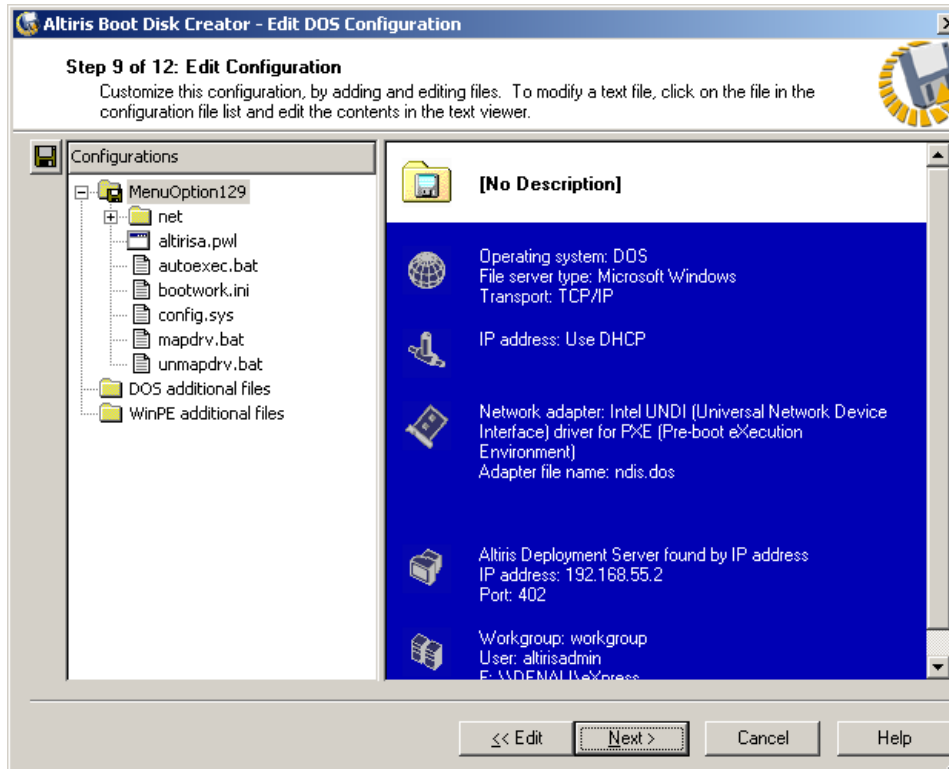


Figure 6-12 The Altiris Boot Disk Creator

5. Right-click the configuration **MenuOption129** and click **Edit Configuration** from the context sensitive pop-up menu. You will see a warning message stating that if you continue, the current contents of the boot image will be rewritten. If you have made any previous changes to the boot image they will be overwritten. Click **Yes** to bypass the warning message if you want to continue.
6. If you want to enter a detailed description for the PXE boot image, you can do so in this window. However, we do not need a detailed description so click **Next** to accept the defaults on the Configuration Name window and continue.
7. Click **Next** to bypass File Server Type window of the Altiris Boot Disk Creator.
8. Step 3 allows you to select the correct network adapter device drivers applicable to your environment. Start by unchecking the check box labeled **Use the Intel UNDI driver for PXE**. Now check the check box labeled **Allow selection of multiple network adapters**. Select from the list, the network adapters you want to use and click **Next** to continue (we have selected the

Broadcom adapters to be compatible with IBM System x and xSeries servers).

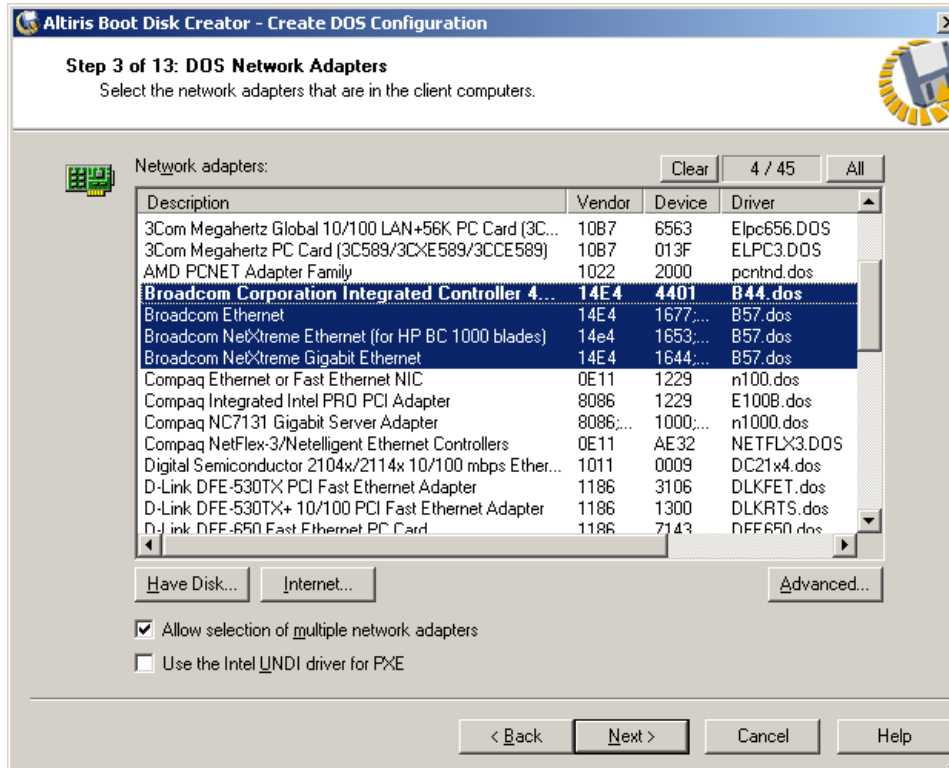


Figure 6-13 Selecting network adapters in the Altiris Boot Disk Creator tool

Attention: If the drivers included with Altiris Deployment Solution do not work with your computer, click **Have Disk** and load the necessary network drivers. Drivers are available on the IBM Support Web site:

<http://www.ibm.com/support/us/>

- The Multiple Network Adapters Load Order windows allows you to change the load order of the network adapter device drivers. Using the **Up** and **Down** buttons we have reordered the list. After reordering your list, click **Next** to continue.

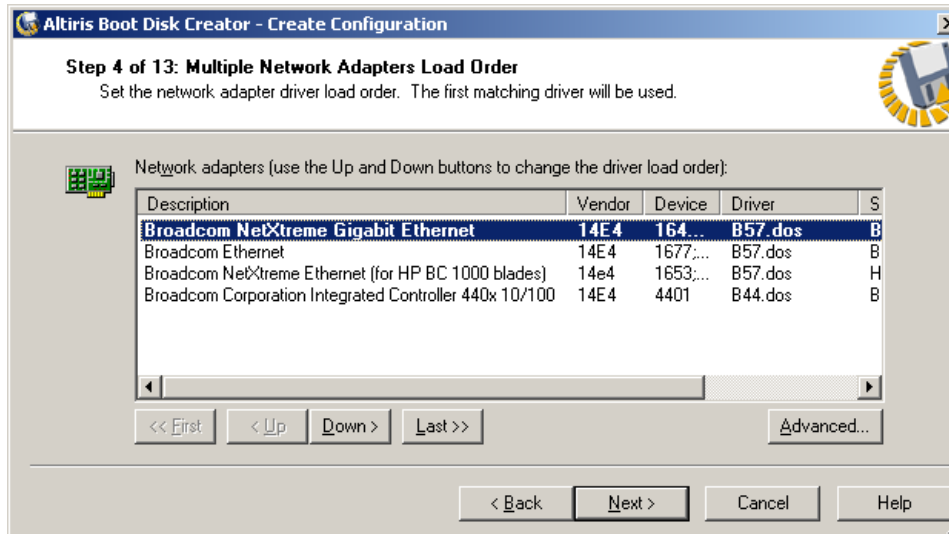


Figure 6-14 Reordered list of network adapter device drivers in the Altiris Boot Disk Creator tool

10. If you want to assign a static IP address to your target computers, select **Use a static IP address** and enter an IP address and Subnet mask. We are using DHCP in our test environment so we accept the defaults and click **Next** to bypass the TCP/IP Protocol Settings window.
11. If you need to use multicasting to locate your Deployment Server, select **Use TCP/IP multicasting to find the Altiris Deployment Server**. In our test environment we have only one Deployment Server and the address was automatically populated correctly so we accepted the default settings. Click **Next** to bypass the Altiris Deployment Server Communication window.
12. The Network Connection window allows you to select the workgroup to connect the target computer(s). You also need to verify the PXE boot image is using the correct *Username* and *Password* to connect to the Deployment Share on the Deployment Server. If these two variables are incorrect, PXE will fail to connect. After verifying the information, click **Next** to bypass the Network Connection window.

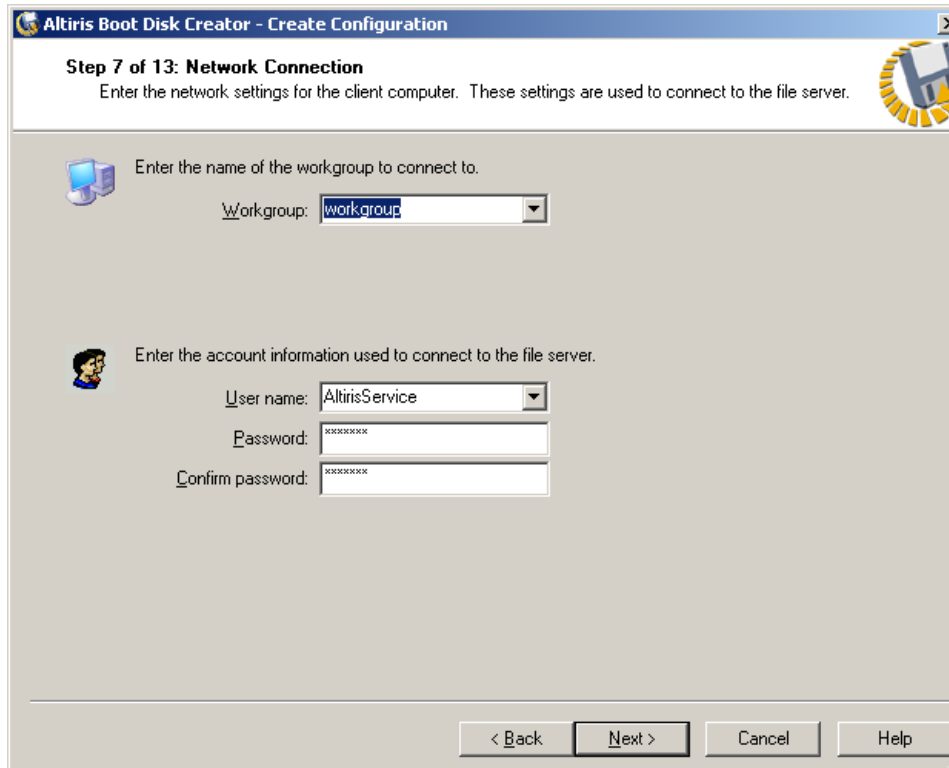


Figure 6-15 The Network Connection window of the PXE Boot Disk Creator

13. On the Network Drive Mappings window you can change the drive mappings to the Deployment Share if necessary. If your network does not support NetBIOS name resolution to IP addresses, you can add an entry to the LMHosts file to map server names to IP addresses. Check the check box labeled **Create an entry in the LMHOSTS file for the Deployment Server file store**. Enter the IP address of the Deployment Server in the IP address text box provided.

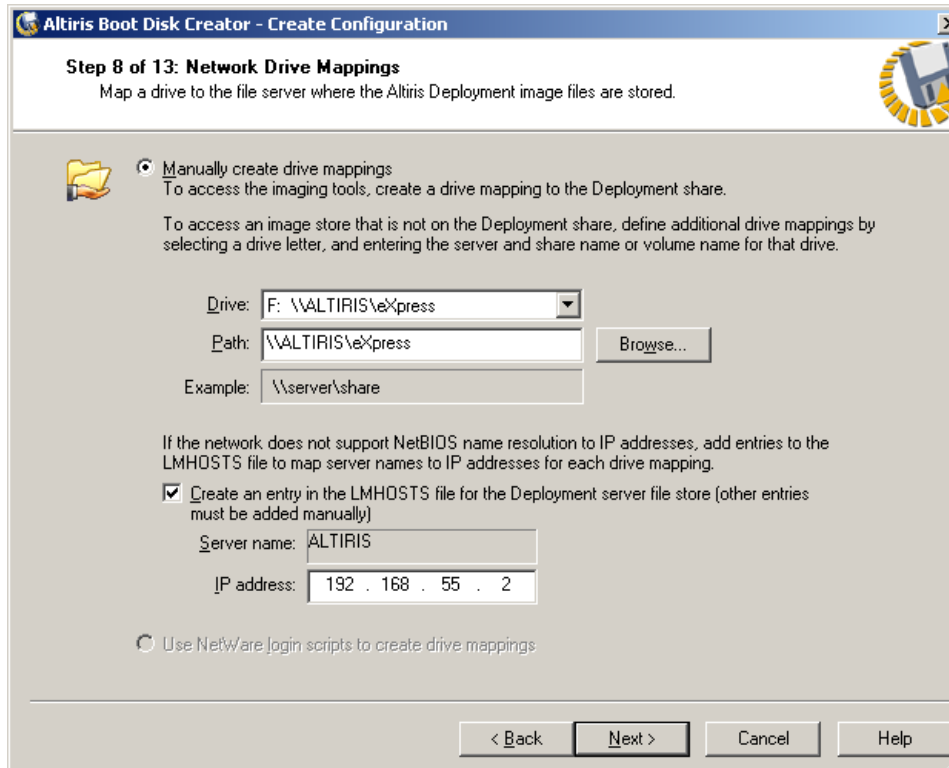


Figure 6-16 The Network Drive Mappings window of the PXE Boot Disk Creator

14. Click **Next** to bypass the Configuration Summary window. This will return you to the window shown in Figure 6-12 on page 185.
15. Click **Next** to move to the next window.
16. Click **Next** to accept the defaults and bypass the Create PXE Boot Image Files window.
17. Click **Finish** to close the Altiris Boot Disk Creator. This will return you to the window shown in Figure 6-11 on page 184. Click **OK** to close the Edit Shared Menu Option window. This will return you to the PXE Configuration Utility. Notice that the **Save** button is enabled after the boot image has been changed. Click **Save** to save the altered boot image.

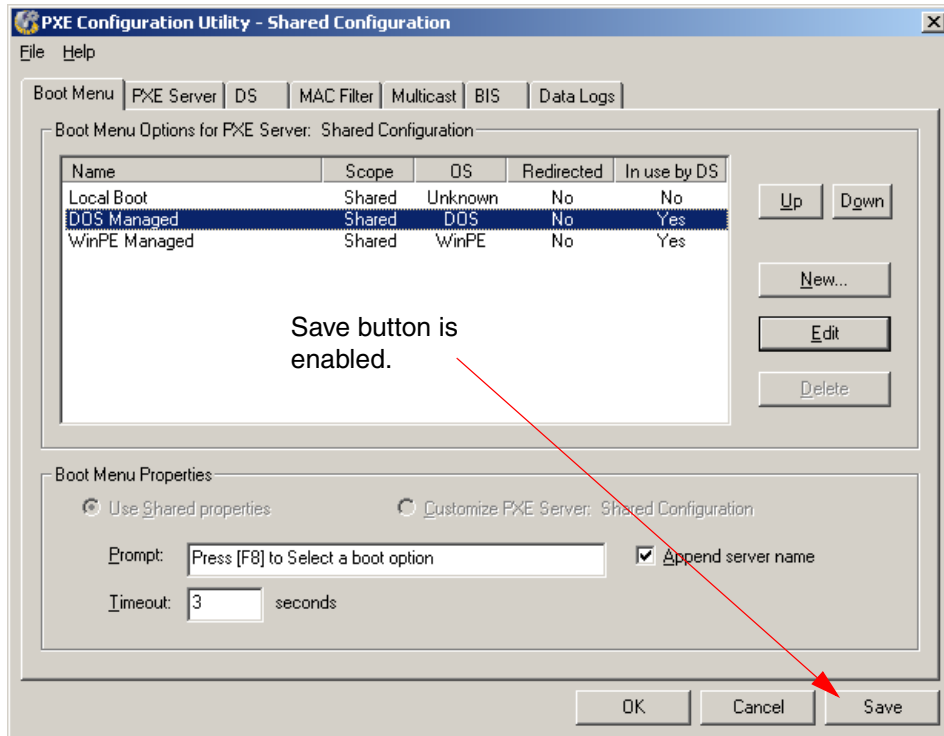


Figure 6-17 The Altiris PXE Configuration Utility with the Save button enabled

Important: Make sure to click **Save** when you have finished altering the boot image. If you do not click Save, your changes will be discarded.

18. Click **OK** to close the PXE Configuration Utility.

Tuning multicast for your environment

You may want to change the threshold for deployment to switch to multicasting rather than unicasting. For example, the default threshold is 4. Deployment Solution will use unicast unless the number of computers you are running the job on is more than or equal to the threshold value.

Follow the steps below if you want to change the threshold value:

1. Open the Altiris Services Configuration Utility by clicking **Start** → **Programs** → **Altiris** → **Deployment Solution** → **Configuration**. The Altiris Deployment Server Configuration Utility will appear as shown below.

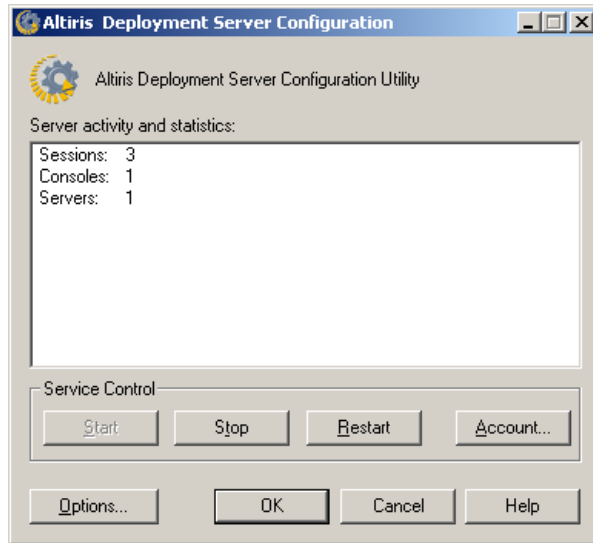


Figure 6-18 The Altiris Deployment Server Configuration utility

2. Click **Options**. The Options window will appear as shown below.

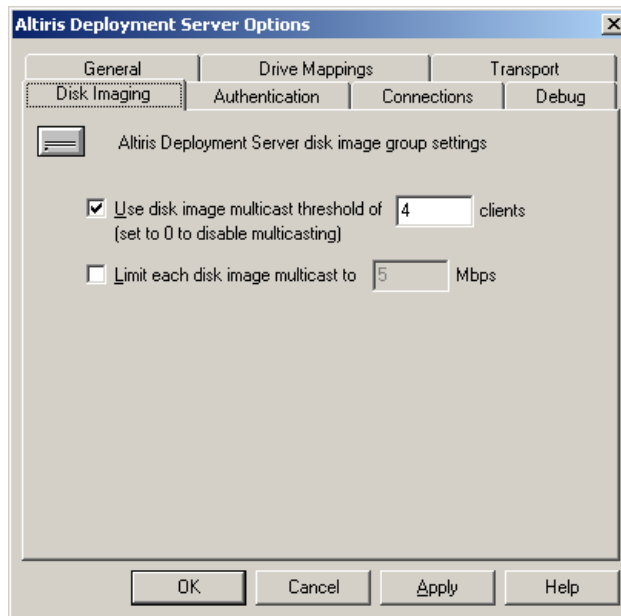


Figure 6-19 The Altiris Deployment Configuration Options window with the Disk Imaging tab shown

3. If you want to change the multicast threshold, check the check box labeled **Use disk image multicast threshold of** and enter the number you want to use as your threshold. Set the number to zero if you want to disable multicasting.

Note: You can also throttle the network usage by checking the check box labeled **Limit each disk image multicast to** and entering a number more appropriate to your environment.

RapiDeploy is more efficient when writing directly to the IP address of the network adapter driver. You can enter a range of IP addresses when using the multicasting feature to speed computer deployment and management. Deployment Solution accesses the range of computers using the defined IP pairs and avoids retrieving the computers through the port and operating system layers.

However, because some network adapter cards do not handle multiple multicast addresses, you can also identify a range of ports to identify these computers. On the first pass Deployment Server accesses the selected computers using the list of IP numbers. On the second pass, Deployment Solution accesses the selected computers using the port numbers or higher level operating system ID's. To change the multicast IP range or port range do the following:

1. Open the Deployment Console.
2. On the menu, click **Tools** → **Options** to display the options window.
3. Click on the **RapiDeploy** tab and change the setting to fit your environment.

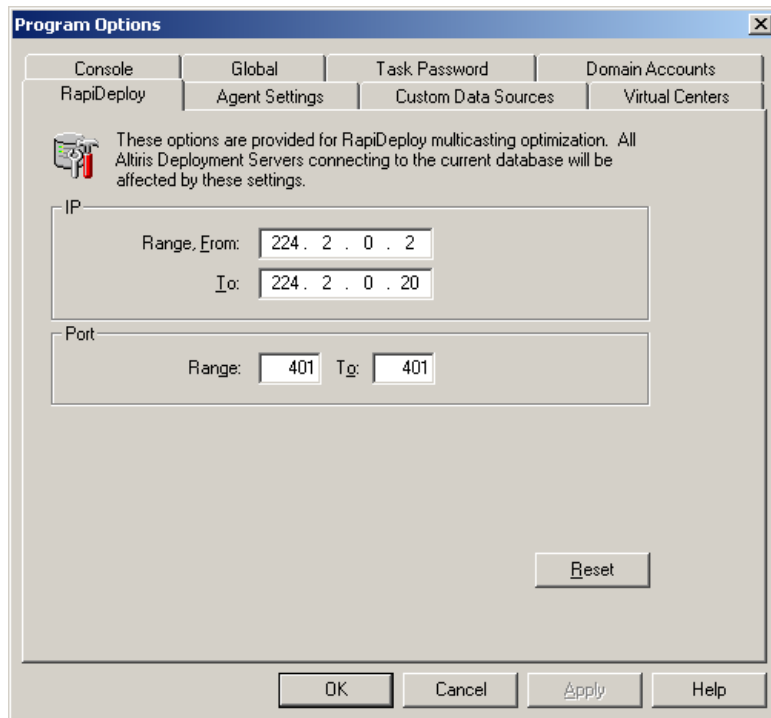


Figure 6-20 The Program Options window with Multicast settings shown

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

For more in depth information regarding multicasting refer to *Altiris Deployment Solution 6.5 Reference Guide*.

6.4 Integrating Sysprep with Deployment Solution

As mentioned previously Altiris Deployment Solution has the ability to integrate with Microsoft Sysprep. The benefits to integrating Sysprep are:

- ▶ Fewer sysprep.inf files to maintain
- ▶ The sysprep.inf files can be saved in a central location
- ▶ Reduced complexity in image management

To fully integrate Sysprep a number of steps must be taken.

1. The Sysprep files must be added to the Deployment Server
2. Global settings must be configured through the Deployment Console

3. A sysprep.inf file must be created (since the creation of a custom Sysprep.inf file is well documented on the internet it will not be covered in this document)

This section will cover the steps outlined above (except for creating the Sysprep.inf file) and also the implementation of sysprep during an image capture and image deployment job.

6.4.1 Integrating the Sysprep files

Sysprep files are installed as part of the initial Altiris Deployment Solution install. If you did not install the Sysprep files, you can do so by initiating the install process and adding a component.

The Component installation option lets you add selected Deployment Server Components- Deployment Console, Deployment Web Console, Altiris PXE Server, and also add Microsoft Sysprep files.

To install Microsoft Sysprep, do the following:

1. To launch the Component installation see 2.1.5, "Component installation" on page 25.
2. Check the check box labeled **Add Microsoft Sysprep files**. Click **Next**.

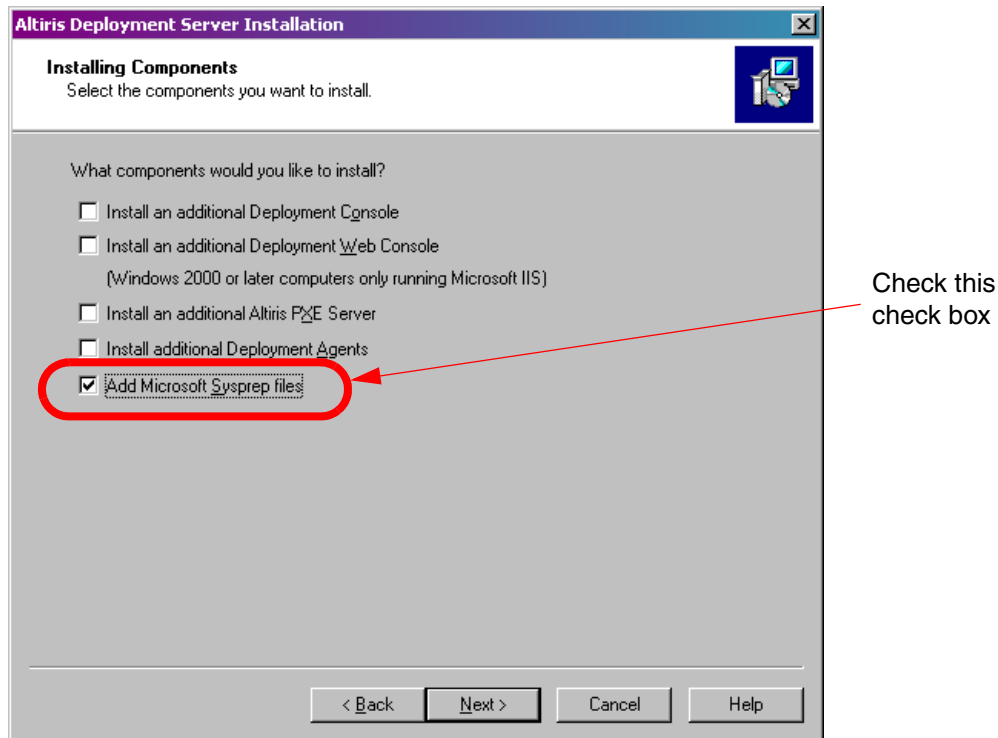


Figure 6-21 The Installing Components selection window

3. Click **Browse** next to the **Windows XP/2003 (Deploy.cab)** text box and browse to the Deploy.cab file that is included on any Windows 2003 installation media. Click **Next**.

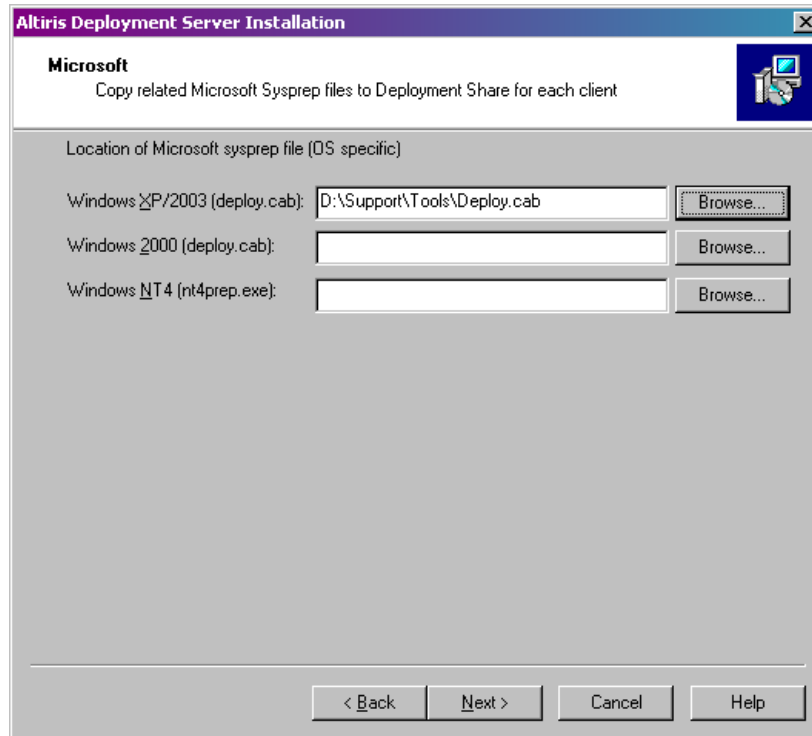


Figure 6-22 The Microsoft window pointing to the location of the Deploy.cab file

4. Click **Install** to begin copying the Sysprep files to the Deployment Server.
5. Click **Finish** when the files have been copied.

Now Microsoft Sysprep has been integrated with Altiris Deployment Solution. However, before using Sysprep its global settings must be configured from the Deployment Console.

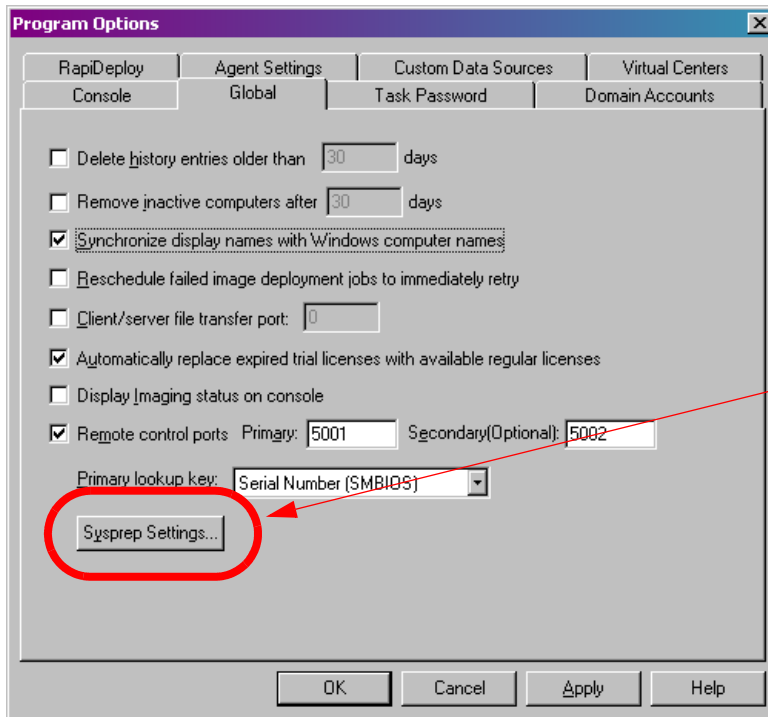
6.4.2 Configuring Sysprep global settings

Before Sysprep can be used in any deployment jobs, its global settings must be configured.

To configure Sysprep's global settings follow the steps below:

1. Open the Deployment Console.
2. Click **Tools** → **Options** on the main menu.

3. Select the **Global** tab and click **Sysprep Settings** as shown in Figure 6-23.



Click the Sysprep Settings button

Figure 6-23 Altiris Deployment Solution Program Options window

4. Click the **Computer Information** tab and enter a user name in the **User name** text box and your organization's name in the **Organization name** text box.

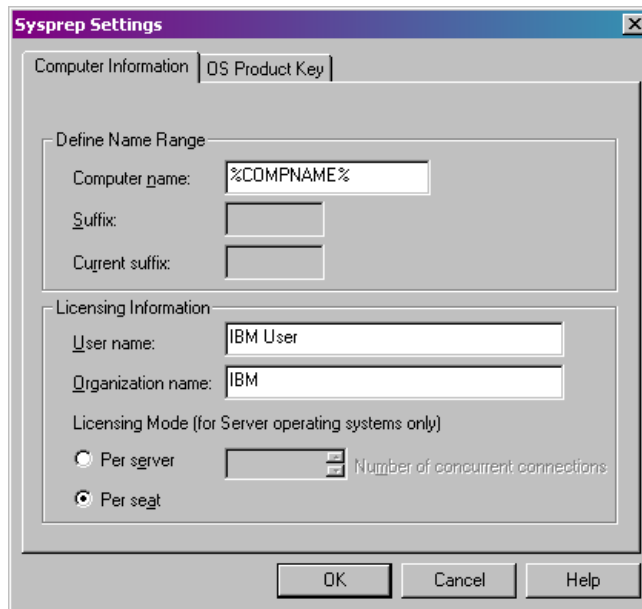


Figure 6-24 The Computer Information tab of the Sysprep Settings window

5. Click the **OS Product Key** tab. On this window you will add operating system product keys for each operating system you plan on imaging using Sysprep. To add a key follow the steps below:
 - a. Select the operating system from the **Operating System** pull-down list.
 - b. Click **Add** and type in the product key you want to use. Click **OK**.

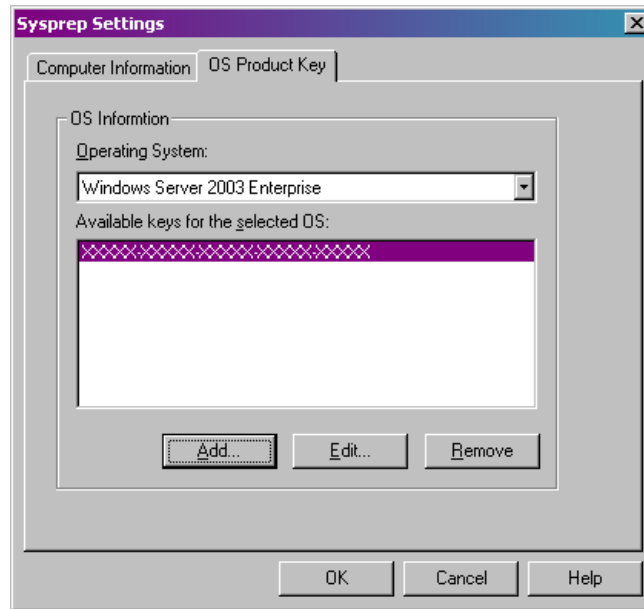


Figure 6-25 The OS Product Key tab of the Sysprep Settings window

6. Click **OK** to close the window.
7. Click **OK** again to close the Options window.

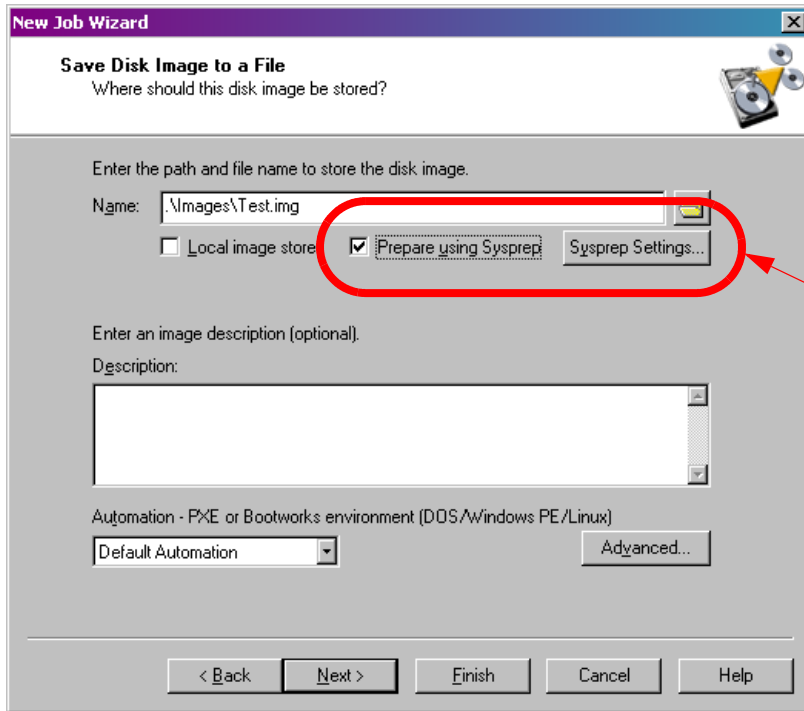
Now Sysprep is configured and can be used in deployment jobs.

6.4.3 Using Sysprep during image capture

During the creation of an image capture job, you have the option to use Sysprep to prepare the image.

To configure Sysprep for image preparation follow the steps below:

1. During the creation of an image capture job, when the Save Disk Image to a File window is shown, check the check box labeled **Prepare using Sysprep** and then click **Sysprep Settings** as shown in Figure 6-26 on page 200.



Check the check box and click the **Sysprep Settings** button

Figure 6-26 The Save Disk Image to a File window

2. On the Answer File / OS tab check the check box labeled **Use following as answer file for Sysprep** and then click the Folder button and browse to your sysprep.inf file. Select the operating system you are imaging from the **Operating System** pull-down list, then select the correct product key from the **Available keys for the selected OS** list box. If you did not add a product key when you integrated Sysprep with Altiris Deployment Solution, click **Add** and enter your product key.

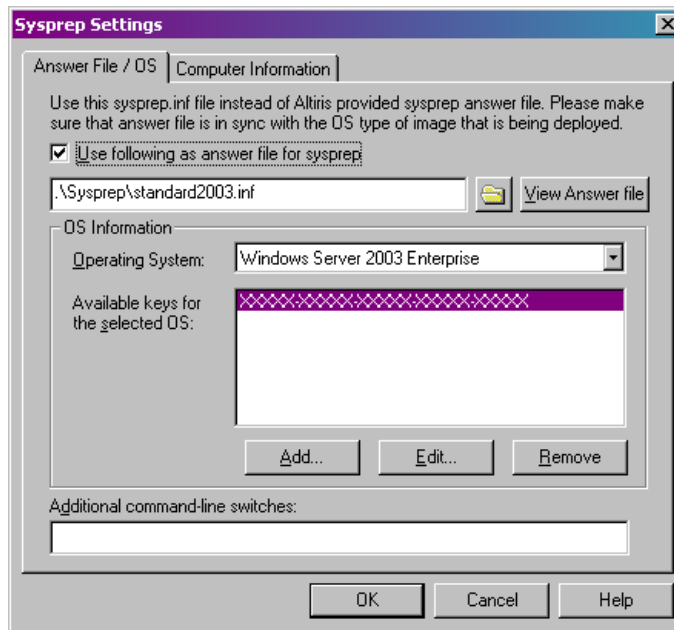


Figure 6-27 The Sysprep Settings window

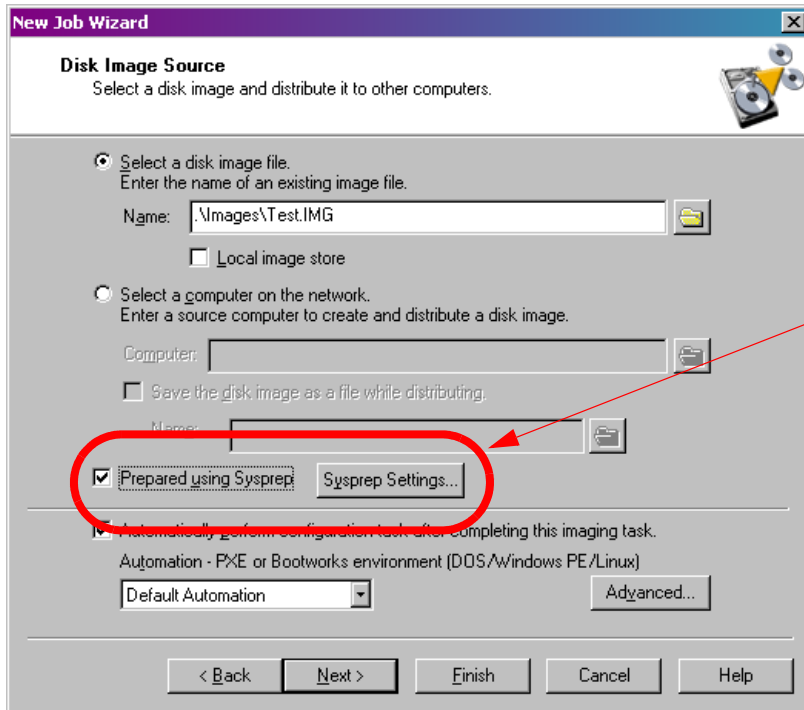
3. Click **OK** to close the Sysprep Settings window and continue with the creation of the image capture job.

When the image capture process is initiated, the Reference Computer will be prepared using Sysprep and will then shutdown.

6.4.4 Using Sysprep during image deployment

Configuring Sysprep for image deployment is the same as configuring Sysprep for image capture.

During the creation of an image deployment job, when the Disk Image Source window loads, check the check box labeled **Prepared using Sysprep** and click **Sysprep Settings** to load the Sysprep Settings window. Configure Sysprep the same as you configured Sysprep in the previous section.



Check the check box and click the **Sysprep Settings** button

Figure 6-28 Disk Image Source window

Now sysprep is configured. When your computer boots for the first time Microsoft Sysprep will prepare the image.

6.5 Creating hardware independent Windows images

A fully hardware-independent image is the ultimate goal of anybody required to maintain a library of operating system images for their environment. However, fully hardware independence is not easily obtained, if even possible with today's technology. Even though it may not be possible to obtain full hardware independence, there are a number of tricks to greatly reduce the number of images needed to support the many different models of System x and xSeries servers.

There are a number of issues associated with creating a hardware-independent image:

- ▶ If the Hardware Abstraction Layers (HAL) or ACPI support are different on your Reference Computer than your target computer the image will fail to load, or worse it could seem to work fine, but could have timing issues.

- ▶ Images created from a Reference Computer with IDE hard drives are not compatible with target computers with SCSI hard drives. The same is true for images created from a Reference Computer with SCSI hard drives and target computers with IDE hard drives.
- ▶ The image must have the correct mass storage device drivers installed to work with a target computer using a different type of storage controller. IBM offers a wide variety of storage controllers among the many System x and xSeries models. While this gives customers more performance options, it also complicates the imaging process. However, with Microsoft's Sysprep utility, you can include all the mass storage device drivers in the disk image allowing your image to work on target computers that have different mass storage controllers.

We have developed a method for creating a computer image that will work for most System x and xSeries server models using device drivers on the latest ServerGuide CD.

Note: Even though this method focuses on the device drivers provided by ServerGuide, the process can easily include additional drivers to make the disk image usable on hardware from other vendors.

The basic flow for creating a hardware independent image is as follows:

1. Install the base Windows operating system onto your Reference Computer.
2. Make any optional changes to the Windows operating system (install components, install applications, change settings, and so forth).
3. Copy the textmode device drivers from the ServerGuide CD to the Reference Computer's hard drive.
4. Create multiple entries in the sysprep.inf file pointing to the various textmode mass storage device drivers.
5. Capture the donor image.
6. Copy the Plug and Play device drivers from the ServerGuide CD to a folder located in the ServerGuide Scripting Toolkit's source tree in the Deployment Share.
7. Create a registry change file that will point the target computer's Windows operating system at the Plug and Play device drivers and save it in the same folder as the Plug and Play device drivers on the Deployment Share.
8. Add a section in the sysprep.inf file to run the registry change file on the target computer when it first boots after being imaged.
9. Create a deployment job to deploy the newly created image

10. Create an additional Run Script deployment task in the deployment job you just created to copy the device drivers and the registry change file to the target computer.
11. Deploy the image.

Note: This method keeps the Plug and Play device drivers separate from the image and stores them in the Deployment Share. When device drivers are updated, simply update them on the Deployment Share. The next time the image is deployed the latest drivers will be copied to the target computer. The registry change file may need to be updated accordingly.

The following sections cover this sequence in more detail.

6.5.1 Using Microsoft Sysprep to achieve hardware independence

Microsoft's Sysprep tool is used to install identical configurations on multiple computers. Sysprep runs Plug and Play detection, creates new security identifiers (SIDs), and runs the MiniSetup Wizard when the target computer first boots after being imaged.

This section assumes working knowledge of Microsoft's System Preparation tool.

Populating the [SysprepMassStorage] section of the Sysprep.inf file

Microsoft's Sysprep tool uses an answer file much like the unattend.txt file, called sysprep.inf. In the sysprep.inf file you can designate the location of textmode mass storage device drivers on the disk image that will be loaded when the target computer boots for the first time after being imaged. The textmode device drivers allow access to the target computer's hard drives while the operating system is being loaded during boot. If the correct drivers are not present or have not been properly designated in the sysprep.inf file the computer will blue-screen and reboot.

This section describes the integration of the ServerGuide textmode device drivers into the donor disk image. This section assumes your Reference Computer has the Windows 2003 Server operating system installed in preparation for creating the donor image.

Populating the [SysprepMassStorage] section of the sysprep.inf file is the most complicated part of achieving hardware independence. This section will guide you through the process of creating a text string to enter into the

[SysprepMassStorage] section, enabling Sysprep to load the correct mass storage device drivers.

Follow the steps below to create an entry in the sysprep.inf file:

1. Power on the Reference Computer.
2. Insert the latest ServerGuide CD into the CD-ROM drive after the Reference Computer has booted into the OS. If the CD is inserted before the computer boots to the OS, the computer will boot to the ServerGuide CD.
3. Create a folder called Drivers in the root of the Reference Computer's system drive (generally C:\)
4. Copy the textmode folder (in the latest release of ServerGuide, the textmode folder for Windows 2003 is located in this directory:
D:\sguide\w2003drv\%oem%\textmode) from the ServerGuide CD to the Drivers folder on the system drive of the Reference Computer (C:\Drivers\).

After the copy process completes you need to create a text string that will be used in the sysprep.inf file, which will load the appropriate mass storage driver when the target computer boots for the first time after being imaged.

Complete the following steps to create a text string to add to the sysprep.inf file:

1. Explore the textmode folder that you copied to your Reference Computer. The textmode folder contains many device drivers and their corresponding .inf files. Open the first .inf file in Notepad.
2. Search through the .inf file and locate a section that lists the ID strings for the mass storage devices supported by this driver. In this case it lists the name of the device followed by the ID string:

```
; models section

[IBM.NTx86.5.2]          ; Section for Windows Server 2003
%SERVERAID4Mx_DESCRIPTION% = NFRD960_Install,
PCI\VEN_1014&DEV_01BD&SUBSYS_02081014
%SERVERAID4Lx_DESCRIPTION% = NFRD960_Install,
PCI\VEN_1014&DEV_01BD&SUBSYS_020E1014
%SERVERAID5i_DESCRIPTION% = NFRD960_Install,
PCI\VEN_1014&DEV_01BD&SUBSYS_02591014
%SERVERAID6M_DESCRIPTION% = NFRD960_Install,
PCI\VEN_9005&DEV_0250&SUBSYS_02791014
%SERVERAID6i_DESCRIPTION% = NFRD960_Install,
PCI\VEN_9005&DEV_0250&SUBSYS_028C1014
%SERVERAID7k_DESCRIPTION% = NFRD960_Install,
PCI\VEN_9005&DEV_0250&SUBSYS_028E1014
```

Figure 6-29 An .inf file with a listing of device IDs

3. Copy the ID portion of the string to a new text document. The text document will be used to build the sysprep entries and will be closed later without saving. Saving or naming the text file is at your discretion.
4. Search through the .inf file for the official name that will be displayed in Windows Device Manager. The name of the device is surrounded by quotation marks in the figure below. Copy the names of the devices supported by this device driver to the text document created in the previous step.

```
; Localizable strings
IBM = "IBM Corporation"
INSTALL_MEDIA_DESCRIPTION = "IBM ServeRAID Device Driver CD/Diskette"
SERVERAID4Mx_DESCRIPTION = "IBM ServeRAID 4Mx Controller"
SERVERAID4Lx_DESCRIPTION = "IBM ServeRAID 4Lx Controller"
SERVERAID5i_DESCRIPTION = "IBM ServeRAID 5i Controller"
SERVERAID6M_DESCRIPTION = "IBM ServeRAID 6M Controller"
SERVERAID6i_DESCRIPTION = "IBM ServeRAID 6i Controller"
SERVERAID7k_DESCRIPTION = "IBM ServeRAID 7k Controller"
```

Figure 6-30 An .inf file with the name that will be displayed in Device Manager

5. Search through the .inf file for a section called [SourceDisksNames]. You need to get the token assigned to the install media (enclosed by percentage signs). Once you have found the token, copy it into the text document you created earlier.

```
[SourceDisksNames]
1 = %INSTALL_MEDIA_DESCRIPTION%,
\WINDOWS\WIN2003\SCSI\IVDRVR\NFRD960.SYS,
```

Figure 6-31 An .inf file with the token assigned to the Source Disk

6. Your text document should now look like the one shown in Figure 6-32 on page 207.

```

%SERVERAID4Mx_DESCRIPTION% = NFRD960_Install,
PCI\VEN_1014&DEV_01BD&SUBSYS_02081014
%SERVERAID4Lx_DESCRIPTION% = NFRD960_Install,
PCI\VEN_1014&DEV_01BD&SUBSYS_020E1014
%SERVERAID5i_DESCRIPTION% = NFRD960_Install,
PCI\VEN_1014&DEV_01BD&SUBSYS_02591014
%SERVERAID6M_DESCRIPTION% = NFRD960_Install,
PCI\VEN_9005&DEV_0250&SUBSYS_02791014
%SERVERAID6i_DESCRIPTION% = NFRD960_Install,
PCI\VEN_9005&DEV_0250&SUBSYS_028C1014
%SERVERAID7k_DESCRIPTION% = NFRD960_Install,
PCI\VEN_9005&DEV_0250&SUBSYS_028E1014

SERVERAID4Mx_DESCRIPTION = "IBM ServeRAID 4Mx Controller"
SERVERAID4Lx_DESCRIPTION = "IBM ServeRAID 4Lx Controller"
SERVERAID5i_DESCRIPTION = "IBM ServeRAID 5i Controller"
SERVERAID6M_DESCRIPTION = "IBM ServeRAID 6M Controller"
SERVERAID6i_DESCRIPTION = "IBM ServeRAID 6i Controller"
SERVERAID7k_DESCRIPTION = "IBM ServeRAID 7k Controller"

INSTALL_MEDIA_DESCRIPTION

```

Figure 6-32 Your text document with the parameters copied from the .inf file

- Using the information in your text document, create one string for each supported mass storage device to add to the sysprep.inf file's [SysprepMassStorage] section. Each string is composed of the following:

```
[ID String]=[Path to the .inf file on the disk image]"\", \"\", \"[mass storage device name]\", \"[token assigned to install media]\"
```

In our example the string for the IBM ServeRAID 7k Controller looks like the following:

```
PCI\VEN_9005&DEV_0250&SUBSYS_028E1014="%SystemDrive%\Drivers\textmode\oemsetup.inf", "\", "IBM ServeRAID 7k Controller", "INSTALL_MEDIA_DESCRIPTION"
```

- Open in Notepad an existing sysprep.inf file and copy the string you created in the previous step and paste it into the Sysprep.inf file under the [SysprepMassStorage] section. If your Sysprep does not contain a [SysprepMassStorage] section then create one.

Note: There are a number of basic sysprep.inf template files included with Altiris Deployment Solution in the Sysprep directory in the Deployment Share.

9. Your Sysprep.inf file's [SysprepMassStorage] section should now look similar to the one shown below.

```
[SysprepMassStorage]
PCI\VEN_1014&DEV_01BD&SUBSYS_02081014=%SystemDrive%\Drivers\oemsetup.inf
", "\", "IBM ServeRAID 4Mx Controller", "INSTALL_MEDIA_DESCRIPTION"
PCI\VEN_1014&DEV_01BD&SUBSYS_020E1014=%SystemDrive%\Drivers\oemsetup.inf
", "\", "IBM ServeRAID 4Lx Controller", "INSTALL_MEDIA_DESCRIPTION"
PCI\VEN_1014&DEV_01BD&SUBSYS_02591014=%SystemDrive%\Drivers\oemsetup.inf
", "\", "IBM ServeRAID 5i Controller", "INSTALL_MEDIA_DESCRIPTION"
PCI\VEN_9005&DEV_0250&SUBSYS_02791014=%SystemDrive%\Drivers\oemsetup.inf
", "\", "IBM ServeRAID 6M Controller", "INSTALL_MEDIA_DESCRIPTION"
PCI\VEN_9005&DEV_0250&SUBSYS_028C1014=%SystemDrive%\Drivers\oemsetup.inf
", "\", "IBM ServeRAID 6i Controller", "INSTALL_MEDIA_DESCRIPTION"
PCI\VEN_9005&DEV_0250&SUBSYS_028E1014=%SystemDrive%\Drivers\oemsetup.inf
", "\", "IBM ServeRAID 7k Controller", "INSTALL_MEDIA_DESCRIPTION"
```

Figure 6-33 The [SysprepMassStorage] section with the added pointer to the drivers

10. If you want to support more mass storage devices, repeat the process for each .inf file in the Textmode directory and add the strings to the sysprep.inf file below the ones you just added. Close and save the sysprep.inf file.
11. Continue by capturing an image of the Reference Computer as shown in 6.3.1, "Capturing a donor image" on page 170. Be sure to point the image capture job at the correct sysprep.inf file.

Note: We have found that in order to load the drivers correctly the sysprep.inf file must be altered *before* creating the image. For example: if you create an image and later alter the sysprep.inf file inside the image by using Altiris Image Explorer the drivers will not load on a newly imaged computer. You must recreate the image after altering the [SysprepMassStorage] section of the sysprep.inf file.

Integrating ServerGuide Plug and Play device drivers

Once the target computer boots for the first time, Sysprep runs Plug and Play detection causing Windows to look for Plug and Play device drivers. Copying the appropriate device drivers to the target computer and making a change in the registry to point to the driver directory will enable Windows to locate xSeries/System x hardware device drivers and install them automatically.

In order for Windows to find the drivers, they must exist on the target computer's hard drive when the target computer boots for the first time after being imaged. There are two ways:

- ▶ One possible way to do this, is to copy the drivers to the Reference Computer and build them in as part of the image. The downside to this approach is the difficulty in updating drivers when updates are released. If you are managing twenty images, and a new driver is released, you would need to recreate all twenty images to include the latest driver set.
- ▶ The alternative is to keep one master copy of the driver set on the Deployment Share and use the Altiris FIRM tool to copy the drivers to the target computer immediately after the image is deployed and before the operating system boots. The FIRM utility is covered in more depth in "Injecting Plug-n-Play device drivers using FIRM" on page 218.

There are two ways to inform Windows of the device drivers location:

- ▶ Adding a line in the sysprep.inf file
- ▶ Making a registry change

In this section we will cover the creation of a registry change file that will be copied to the target computer and run when the computer boots for the first time after being imaged.

To prepare the ServerGuide Plug and Play device drivers and to create a registry change file, follow the steps below (this section assumes you are copying device drivers for Windows Server 2003):

1. Import the Windows Server 2003 ServerGuide Plug and Play device drivers into the SGTK source tree as shown in "Add device driver files" on page 40.
2. Open a command prompt and issue the following command to put the list of files in the w23_drv directory in a text file:

```
dir <path to SGTK source tree>\drvs\w23_drv /b > <path to SGTK source tree>\drvs\w23_drv\DevicePath.txt
```

where *<path to SGTK source tree>* is the path to the ServerGuide Scripting Toolkit's source tree located in the Deployment Share.

3. Open Windows Explorer and navigate to the w23_drv folder in the SGTK source tree. Open the DevicePath.txt file in Notepad. The contents should look similar to Figure 6-34 on page 210.

```
act
act2
actj
actj2
asf
asm
asm2
atirn
bc
dds
e1
e2
hrsas
...
```

Figure 6-34 The DevicePath.txt file with the basic folder structure of the w23_drv directory

4. Next, open each directory in the w23_drv folder and drill down to the .inf file belonging to the driver for the correct operating system version (e.g. Windows 2000, Windows Server 2003 32-bit, Windows Server 2003 64-bit). Once you find the .inf file add the rest of the path to the appropriate line.

If you cannot find the .inf file or if the directory contains only an executable file remove the folder name from the text document. The text file should now look similar to Figure 6-35.

```
act
act2
actj
actj2
asf
asm\Win2000
asm2\Win2000
atirn\Driver\2KXP_INF
bc\IA32
dds
e1
e2
hrsas
...
```

Figure 6-35 Partial contents of the DevicePath.txt file after adding paths to the .inf files

5. After you have completely gone through the w23_drv folder and updated the DevicePath.txt document to point to all the .inf files, add the following, which points to the eventual destination on the target computer, to the beginning of each line of text:

```
;%SystemDrive%\Drivers\
```

Now the DevicePath.txt file should look similar to Figure 6-36.

```
;%SystemDrive%\Drivers\act
;%SystemDrive%\Drivers\act2
;%SystemDrive%\Drivers\actj
;%SystemDrive%\Drivers\actj2
;%SystemDrive%\Drivers\asf
;%SystemDrive%\Drivers\asm\Win2000
;%SystemDrive%\Drivers\asm2\Win2000
;%SystemDrive%\Drivers\atirn\Driver\2KXP_INF
;%SystemDrive%\Drivers\bc\IA32
;%SystemDrive%\Drivers\dds
;%SystemDrive%\Drivers\e1
;%SystemDrive%\Drivers\e2
;%SystemDrive%\Drivers\hrsas
...
```

Figure 6-36 Partial contents of the DevicePath.txt file after adding the root folder to each line

6. Finally, remove the line feeds to create one continuous line of text and delete the semicolon at the very beginning of the line. The final result should look like the text file shown in Figure 6-37 (word wrap is enabled to see the entire line).

```
%SystemDrive%\Drivers\act;%SystemDrive%\Drivers\act2;%SystemDrive%\Drivers\actj;%SystemDrive%\Drivers\actj2;%SystemDrive%\Drivers\asf;%SystemDrive%\Drivers\asm\Win2000;%SystemDrive%\Drivers\asm2\Win2000;%SystemDrive%\Drivers\atirn\Driver\2KXP_INF;%SystemDrive%\Drivers\bc\IA32;%SystemDrive%\Drivers\dds;%SystemDrive%\Drivers\e1;%SystemDrive%\Drivers\e2;%SystemDrive%\Drivers\hrsas...
```

Figure 6-37 Partial contents of the DevicePath.txt file after the continuous string has been created

7. Save the DevicePath.txt file.

Now that the text string pointing to the Plug and Play device drivers has been created, you can use that string to create a registry change file. Follow the steps outlined below to make a registry change file.

1. Open the Windows Registry Editor by clicking **Start** → **Run** and typing **Regedit**.

Attention: Backup up the Windows Registry before making any changes.

2. Drill down to the following registry key:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
3. Select the key and then double-click **DevicePath** in the details pane. The Edit String window will appear as shown in Figure 6-38.

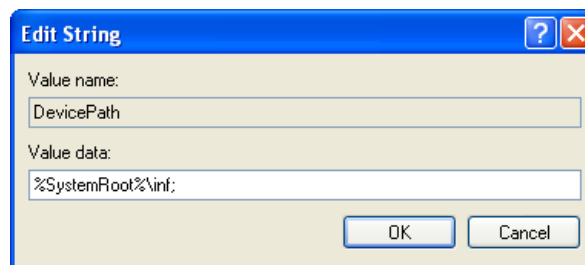


Figure 6-38 Edit String window in the Windows Registry Editor

4. Copy the entire contents of the DevicePath.txt file you created to the clipboard and paste after the existing data in the Value Data text box. The Value Data should now look like Figure 6-39.

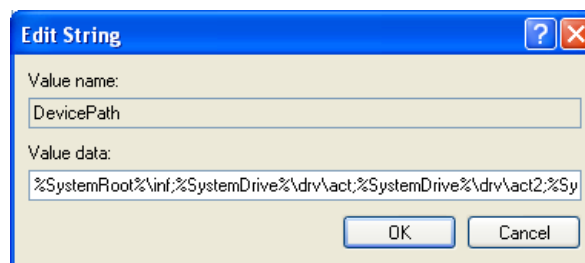


Figure 6-39 Edit String window in the Windows Registry Editor with the added device path string

5. Click **OK**.
6. Click **File** → **Export** from Regedit's main menu to export the DevicePath key.

7. Save the .reg file in the w23_drv folder in the SGTK source tree as DvcPath.reg.
8. Restore the DevicePath registry key to its original value by deleting everything after %SystemRoot%\inf; and close the Windows Registry Editor.
9. Open the DvcPath.reg file in Notepad. It will be a very large text file and should look similar to the one shown below (the numeric values will be different).

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion]

```
"DevicePath"=hex(2):25,00,53,00,79,00,73,00,74,00,65,00,6d,00,52,00,6f,00,6f,\
00,74,00,25,00,5c,00,69,00,6e,00,66,00,3b,00,25,00,53,00,79,00,73,00,74,00,\
65,00,6d,00,44,00,72,00,69,00,76,00,65,00,25,00,5c,00,70,00,6e,00,70,00,5c,\
00,30,00,32,00,30,00,3b,00,25,00,53,00,79,00,73,00,74,00,65,00,6d,00,44,00,\
72,00,69,00,76,00,65,00,25,00,5c,00,70,00,6e,00,70,00,5c,00,30,00,31,00,39,\
00,3b,00,25,00,53,00,79,00,73,00,74,00,65,00,6d,00,44,00,72,00,69,00,76,00,\
65,00,25,00,5c,00,70,00,6e,00,70,00,5c,00,30,00,31,00,38,00,3b,00,25,00,53,\
00,79,00,73,00,74,00,65,00,6d,00,44,00,72,00,69,00,76,00,65,00,25,00,5c,00,\
70,00,6e,00,70,00,5c,00,30,00,31,00,37,00,3b,00,25,00,53,00,79,00,73,00,74,\
00,65,00,6d,00,44,00,72,00,69,00,76,00,65,00,25,00,5c,00,70,00,6e,00,70,00,\
5c,00,30,00,31,00,36,00,3b,00,25,00,53,00,79,00,73,00,74,00,65,00,6d,00,44,\
00,72,00,69,00,76,00,65,00,25,00,5c,00,70,00,6e,00,70,00,5c,00,30,00,31,00,\
35,00,3b,00,25,00,53,00,79,00,73,00,74,00,65,00,6d,00,44,00,72,00,69,00,76,\
00,65,00,25,00,5c,00,70,00,6e,00,70,00,5c,00,30,00,31,00,34,00,3b,00,25,00,\
53,00,79,00,73,00,74,00,65,00,6d,00,44,00,72,00,69,00,76,00,65,00,25,00,5c,\
00,70,00,6e,00,70,00,5c,00,30,00,31,00,33,00,3b,00,25,00,53,00,79,00,73,00,\
74,00,65,00,6d,00,44,00,72,00,69,00,76,00,65,00,25,00,5c,00,70,00,6e,00,70,\
00,5c,00,30,00,31,00,32,00,3b,00,25,00,53,00,79,00,73,00,74,00,65,00,6d,00,\
44,00,72,00,69,00,76,00,65,00,25,00,5c,00,70,00,6e,00,70,00,5c,00,30,00,31,\
00,31,00,3b,00,25,00,53,00,79,00,73,00,74,00,65,00,6d,00,44,00,72,00,69,00,\
76,00,65,00,25,00,5c,00,70,00,6e,00,70,00,5c,00,30,00,31,00,30,00,3b,00,25,\
00,53,00,79,00,73,00,74,00,65,00,6d,00,44,00,72,00,69,00,76,00,65,00,25,00,\
5c,00,70,00,6e,00,70,00,5c,00,30,00,30,00,39,00,3b,00,25,00,53,00,79,00,73,\
00,74,00,65,00,6d,00,44,00,72,00,69,00,76,00,65,00,25,00,5c,00,70,00,6e,00,\
70,00,5c,00,30,00,30,00,38,00,3b,00,25,00,53,00,79,00,73,00,74,00,65,00,6d,\
00,44,00,72,00,69,00,76,00,65,00,25,00,5c,00,70,00,6e,00,70,00,5c,00,30,00,\
30,00,37,00,3b,00,25,00,53,00,79,00,73,00,74,00,65,00,6d,00,44,00,72,00,69,\
00,76,00,65,00,25,00,5c,00,70,00,6e,00,70,00,5c,00,30,00,30,00,36,00,3b,00,\
25,00,53,00,79,00,73,00,74,00,65,00,6d,00,44,00,72,00,69,00,76,00,65,00,25,\
00,5c,00,70,00,6e,00,70,00,5c,00,30,00,30,00,35,00,3b,00,25,00,53,00,79,00,\
73,00,74,00,65,00,6d,00,44,00,72,00,69,00,76,00,65,00,25,00,5c,00,70,00,6e,\
00,70,00,5c,00,30,00,30,00,34,00,3b,00,25,00,53,00,79,00,73,00,74,00,65,00,\
6d,00,44,00,72,00,69,00,76,00,65,00,25,00,5c,00,70,00,6e,00,70,00,5c,00,30,\
00,30,00,33,00,3b,00,25,00,53,00,79,00,73,00,74,00,65,00,6d,00,44,00,72,00,\
69,00,76,00,65,00,25,00,5c,00,70,00,6e,00,70,00,5c,00,30,00,30,00,32,00,3b,\
00,25,00,53,00,79,00,73,00,74,00,65,00,6d,00,44,00,72,00,69,00,76,00,65,00,\
25,00,5c,00,70,00,6e,00,70,00,5c,00,30,00,30,00,31,00,00,00  

"MediaPathUnexpanded"=hex(2):25,00,53,00,79,00,73,00,74,00,65,00,6d,00,52,00,\
6f,00,6f,00,74,00,25,00,5c,00,4d,00,65,00,64,00,69,00,61,00,00,00  

"SM_GamesName"="Games"  

"SM_ConfigureProgramsName"="Set Program Access and Defaults"  

"ProgramFilesDir"="C:\\Program Files"  

"CommonFilesDir"="C:\\Program Files\\Common Files"  

"ProductId"="76487-OEM-0011903-00107"  

"WallPaperDir"=hex(2):25,00,53,00,79,00,73,00,74,00,65,00,6d,00,52,00,6f,00,6f,\
...
```

Figure 6-40 The partial contents of the DvcPath.reg file

10. The only portion needed for the registry key change file is the name of the key and the values for the DevicePath portion of the key. With Notepad, modify the DvcPath.reg file by deleting all text after the last value of the "DevicePath" portion. Your DvcPath.reg file should look similar to the one shown below (the numeric values will be different).

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion]
"DevicePath"=hex(2):25,00,53,00,79,00,73,00,74,00,65,00,6d,00,52,00,6f,00,6f,\
00,74,00,25,00,5c,00,69,00,6e,00,66,00,3b,00,25,00,53,00,79,00,73,00,74,00,\
65,00,6d,00,44,00,72,00,69,00,76,00,65,00,25,00,5c,00,70,00,6e,00,70,00,5c,\
00,30,00,32,00,30,00,3b,00,25,00,53,00,79,00,73,00,74,00,65,00,6d,00,44,00,\
72,00,69,00,76,00,65,00,25,00,5c,00,70,00,6e,00,70,00,5c,00,30,00,31,00,39,\
00,3b,00,25,00,53,00,79,00,73,00,74,00,65,00,6d,00,44,00,72,00,69,00,76,00,\
65,00,25,00,5c,00,70,00,6e,00,70,00,5c,00,30,00,31,00,38,00,3b,00,25,00,53,\
00,79,00,73,00,74,00,65,00,6d,00,44,00,72,00,69,00,76,00,65,00,25,00,5c,00,\
70,00,6e,00,70,00,5c,00,30,00,31,00,37,00,3b,00,25,00,53,00,79,00,73,00,74,\
00,65,00,6d,00,44,00,72,00,69,00,76,00,65,00,25,00,5c,00,70,00,6e,00,70,00,\
5c,00,30,00,31,00,36,00,3b,00,25,00,53,00,79,00,73,00,74,00,65,00,6d,00,44,\
00,72,00,69,00,76,00,65,00,25,00,5c,00,70,00,6e,00,70,00,5c,00,30,00,31,00,\
35,00,3b,00,25,00,53,00,79,00,73,00,74,00,65,00,6d,00,44,00,72,00,69,00,76,\
00,65,00,25,00,5c,00,70,00,6e,00,70,00,5c,00,30,00,31,00,34,00,3b,00,25,00,\
53,00,79,00,73,00,74,00,65,00,6d,00,44,00,72,00,69,00,76,00,65,00,25,00,5c,\
00,70,00,6e,00,70,00,5c,00,30,00,31,00,33,00,3b,00,25,00,53,00,79,00,73,00,\
74,00,65,00,6d,00,44,00,72,00,69,00,76,00,65,00,25,00,5c,00,70,00,6e,00,70,\
00,5c,00,30,00,31,00,32,00,3b,00,25,00,53,00,79,00,73,00,74,00,65,00,6d,00,\
44,00,72,00,69,00,76,00,65,00,25,00,5c,00,70,00,6e,00,70,00,5c,00,30,00,31,\
00,31,00,3b,00,25,00,53,00,79,00,73,00,74,00,65,00,6d,00,44,00,72,00,69,00,\
76,00,65,00,25,00,5c,00,70,00,6e,00,70,00,5c,00,30,00,31,00,30,00,3b,00,25,\
00,53,00,79,00,73,00,74,00,65,00,6d,00,44,00,72,00,69,00,76,00,65,00,25,00,\
5c,00,70,00,6e,00,70,00,5c,00,30,00,30,00,39,00,3b,00,25,00,53,00,79,00,73,\
00,74,00,65,00,6d,00,44,00,72,00,69,00,76,00,65,00,25,00,5c,00,70,00,6e,00,\
70,00,5c,00,30,00,30,00,38,00,3b,00,25,00,53,00,79,00,73,00,74,00,65,00,6d,\
00,44,00,72,00,69,00,76,00,65,00,25,00,5c,00,70,00,6e,00,70,00,5c,00,30,00,\
30,00,37,00,3b,00,25,00,53,00,79,00,73,00,74,00,65,00,6d,00,44,00,72,00,69,\
00,76,00,65,00,25,00,5c,00,70,00,6e,00,70,00,5c,00,30,00,30,00,36,00,3b,00,\
25,00,53,00,79,00,73,00,74,00,65,00,6d,00,44,00,72,00,69,00,76,00,65,00,25,\
00,5c,00,70,00,6e,00,70,00,5c,00,30,00,30,00,35,00,3b,00,25,00,53,00,79,00,\
73,00,74,00,65,00,6d,00,44,00,72,00,69,00,76,00,65,00,25,00,5c,00,70,00,6e,\
00,70,00,5c,00,30,00,30,00,34,00,3b,00,25,00,53,00,79,00,73,00,74,00,65,00,\
6d,00,44,00,72,00,69,00,76,00,65,00,25,00,5c,00,70,00,6e,00,70,00,5c,00,30,\
00,30,00,33,00,3b,00,25,00,53,00,79,00,73,00,74,00,65,00,6d,00,44,00,72,00,\
69,00,76,00,65,00,25,00,5c,00,70,00,6e,00,70,00,5c,00,30,00,30,00,32,00,3b,\
00,25,00,53,00,79,00,73,00,74,00,65,00,6d,00,44,00,72,00,69,00,76,00,65,00,\
25,00,5c,00,70,00,6e,00,70,00,5c,00,30,00,30,00,31,00,00,00
```

Figure 6-41 The complete contents of the DvcPath.reg file

11. Save and close the DvcPath.reg file. Close Regedit.

You have now finished creating a registry change file. When copied to the target computer and run, the file will change the registry to point to the Plug and Play device drivers that will be copied to the target computer's hard drive during the imaging process.

To run the registry change file on the target computer a small change must be made in the sysprep.inf file that will be used when the target computer reboots. Follow the steps below to modify the sysprep.inf file.

1. Open the sysprep.inf file you will be using in Notepad.
2. Add the following portion to the sysprep.inf file:

```
[GuiRunOnce]
Command0="regedit.exe /s C:\Drivers\DvcPath.reg"
```

Your sysprep.inf should look similar to the one below.

```

[Unattended]
    OemSkipEula=Yes
    InstallFilesPath=C:\sysprep\i386
[GuiUnattended]
    AdminPassword=*
    EncryptedAdminPassword=NO
    AutoLogon=Yes
    AutoLogonCount=1
    OEMSkipRegional=1
    OEMDuplicatorstring="Windows 2003 ES"
    TimeZone=Your Time Zone
    OemSkipWelcome=1
[UserData]
    ProductKey=XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
    FullName="W2003ES"
    OrgName="Your Org Name"
    ComputerName=*
[GuiRunOnce]
    Command0="regedit.exe /s C:\Drivers\DvcPath.reg"
[Display]
    BitsPerPel=32
    Xresolution=1024
    YResolution=768
[LicenseFilePrintData]
    AutoMode=PerServer
    AutoUsers=5
[SetupMgr]
    DistFolder=C:\sysprep\i386
    DistShare=windist
[Identification]
    JoinWorkgroup=WORKGROUP
[Networking]
    InstallDefaultComponents=Yes
...

```

Figure 6-42 The contents of the sysprep.inf file with the [GuiRunOnce] section added

3. Save and close the sysprep.inf file.

Now the sysprep.inf file is complete. Finally we need to create a deployment task to inject the device drivers and the registry change file to the target computer using the FIRM utility.

Injecting Plug-n-Play device drivers using FIRM

The File System Independent Resource Management (FIRM) utility is part of Altiris Deployment Solution. The benefit of FIRM is that it gives you basic file access to all FAT, NTFS, and EXT2 file systems on your hard disk, regardless of the version of DOS you are running. This is important for copying files between operating systems such as registry files, configuration files, or any file that a user may want to copy from DOS to an NTFS or EXT2 partition after the machine has been imaged but before it boots.

This is an advanced Altiris utility feature. You don't have to use it to perform normal management tasks. FIRM serves as an interface between DOS and the partitions on hard disks. You can use FIRM commands to manage both DOS disks and FIRM drives (FAT, NTFS, and EXT2).

With FIRM, it's easy to access and manage both BootWorks and production partitions. When you are in DOS, you can see only the BootWorks and FAT partitions. When you are in production mode, you cannot see the BootWorks partition. FIRM allows you to access both BootWorks and production partitions.

Note: If you are using RapiDeploy as a stand-alone product without Deployment Solution, automation partitions are not available.

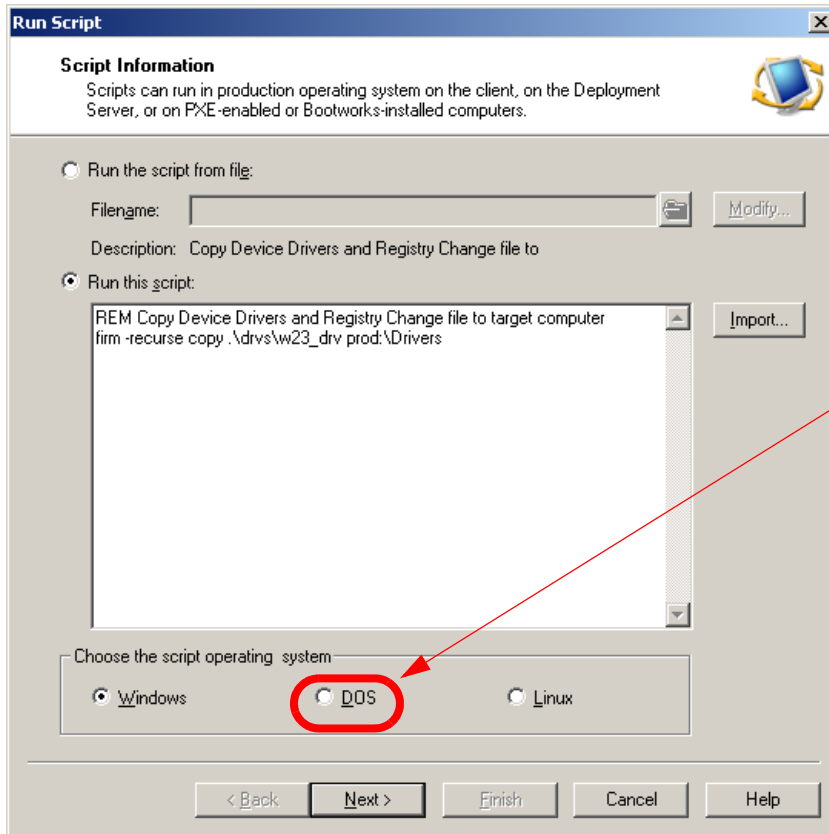
For more information about FIRM refer to the *Altiris Deployment Solution 6.5 Reference Guide*.

To configure a deployment task to copy in device drivers and the registry change file using FIRM follow the steps outlined below:

1. In the Deployment Console select an existing image deployment job.
2. In the details pane select the job and click **Add** to add a new deployment task.
3. Select **Run Script** from the pop-up menu.
4. Add the following line to the Run Script deployment task:

```
firm -recurse copy .\drvs\w23_drv prod:\Drivers
```

Finally, select the **DOS** radio button to use DOS as the operating system in which the script will run.



Select DOS for the OS in which to run the script.

Figure 6-43 The contents of the deployment task to inject device drivers and the registry change file

5. Click **Next**. Click **Finish** to close the window.

This completes the method for creating hardware independent images. Deploy your deployment job onto a target computer and after the imaging process completes the computer will download the device drivers and the registry change file. When the target computer boots the sysprep.inf file will run the registry change file (DvcPath.reg) instructing Windows where to look for Plug and Play device drivers.

When your target computer boots all Plug and Play devices should be discovered and the device drivers should be loaded. If the Device Manager of your target computer has yellow bang symbols (!), the correct drivers were not available. Download the correct device drivers from the hardware manufacturer and add them to the Plug and Play device drivers folder on the Deployment Share. Finally, create a new registry change file to incorporate the added drivers.

6.6 Imaging with Windows PE

Microsoft Windows Preinstallation Environment (Windows PE or WinPE) is a replacement for MS-DOS. Windows PE is a stripped down Windows operating system that is based on the Windows XP and Windows 2003 kernels. Windows PE is supported on both desktop computers and servers.

Note: Enterprise Agreement and Software Assurance customers will receive Windows PE as part of their license agreements. Also, Windows PE can be licensed by all Microsoft Certified Partners, IHVs, ISVs, and ODMs.

Some of the advantages to using Windows PE over MS-DOS as your PXE boot disk image are listed below:

- ▶ Provides more powerful maintenance and troubleshooting tools than available in MS-DOS
- ▶ Provides access to NTFS file-system partitions with the ability to format partitions with NTFS
- ▶ Provides access to network shares
- ▶ Provides the ability to insert 32-bit and 64-bit device drivers into an existing Windows PE PXE boot disk image to add additional support for mass-storage devices, video adapters, and other devices
- ▶ Imaging with Windows PE is generally ten times faster than when using MS-DOS

Note: Because the Windows PE PXE boot disk image can be greater than 100 MB in size it takes longer to download it to the target computer(s) than a MS-DOS PXE boot image. If your network infrastructure is gigabit the additional time is negligible; however, if your network infrastructure is slower this could impact performance.

Attention: There is a defect in Windows PE that can cause abnormal download times on certain computers. We have seen this primarily, but not exclusively, on Blade computers. To read more about the defect and possible workarounds view the following URL:

<http://support.microsoft.com/?kbid=906425>

Adding Windows PE files to Altiris Deployment Solution

If you did not add the Windows PE files as a pre-boot operating system when you installed Altiris Deployment Solution you will need to add the files now.

To add the Windows PE files follow the steps outlined below:

1. Open Deployment Console.
2. On the main menu click **Tools** → **Boot Disk Creator** to open the Boot Disk Creator Wizard. If the Boot Disk Creator Wizard splash window appears, select **Go to the Boot Disk Creator interface** and click **OK**.
3. On the main menu of the Boot Disk Creator Wizard, click **Tools** → **Install Pre-Boot Operating Systems**.
4. On the Install Pre-boot Operating System Files window click **Install** in the Windows PE section.
5. Insert into your CD-ROM drive, the Windows PE 2005 CD. On the Windows PE CD window type the path to your CD-ROM drive and click **Next**.
6. Insert into your CD-ROM drive, your Windows 2003 with integrated SP1 CD (volume edition is preferred). On the Windows CD window type the path to your CD-ROM drive and click **Next**.
7. Click **Finish** to close the Install Complete window. Click **Close** to close the Install Pre-boot Operating System Files window. Close the Boot Disk Creator.

Creating a Windows PE boot disk

Now that you have installed the Windows PE files to Deployment Solution, you can create a Windows PE PXE boot disk image.

To create a Windows PE PXE boot disk image follow the steps outline below:

1. Open the Deployment Console.
2. On the main menu, click **Tools** → **PXE Configuration** to open the PXE Configuration Utility. On the Boot Menu tab click **New** to open the New Menu Shared Option window.
3. Give the PXE boot disk image a meaningful name and select **WinPE** in the Operating System section. Click **Create Boot Image**.

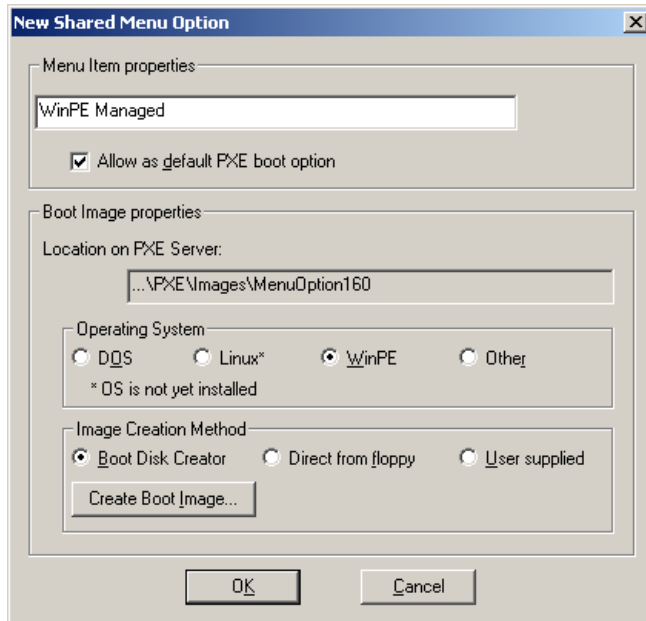


Figure 6-44 The New Shared Menu Option window

4. Enter a detailed description in the Configuration Name window and click **Next**.
5. On the Windows PE Network Adapters window leave the check box labeled **Auto-detect all network adapters** checked. If you want to add additional network drivers click **Have Disk**. Click **Next**.
6. If you want to assign a static IP address to your target computers, select **Use a static IP address** and enter an IP address and Subnet mask. We are using DHCP in our test environment so we accept the defaults and click **Next** to bypass the TCP/IP Protocol Settings window.
7. If you need to use multicasting to locate your Deployment Server select **Use TCP/IP multicasting to find the Altiris Deployment Server**. In our test environment we have only one Deployment Server and the address was automatically populated correctly so we accepted the default settings. Click **Next** to bypass the Altiris Deployment Server Communication window.
8. The Network Connection window allows you to select the workgroup to connect the target computer(s). You also need to verify the PXE boot image is using the correct *Username* and *Password* to connect to the Deployment Share on the Deployment Server. If these two variables are incorrect, PXE will fail to connect. After verifying the information, click **Next** to bypass the Network Connection window.

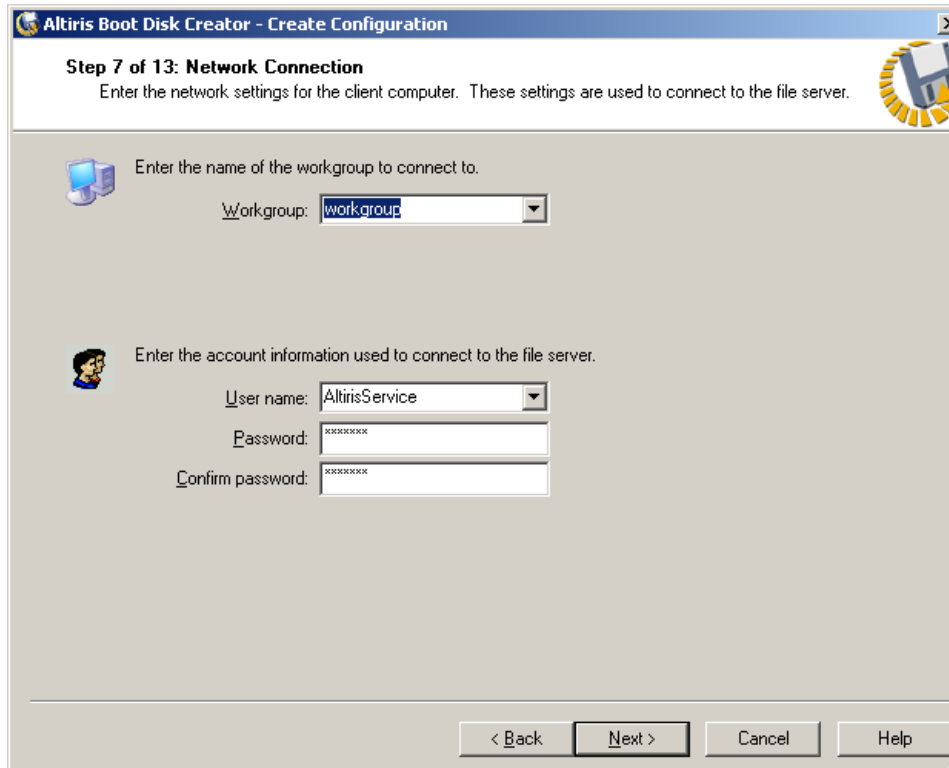


Figure 6-45 The Network Connection window of the PXE Boot Disk Creator

9. On the Network Drive Mappings window you can change the drive mappings to the Deployment Share if necessary. If your network does not support NetBIOS name resolution to IP addresses, you can add an entry to the LMHosts file to map server names to IP addresses. Check the check box labeled **Create an entry in the LMHOSTS file for the Deployment Server file store**. Enter the IP address of the Deployment Server in the IP address text box provided.

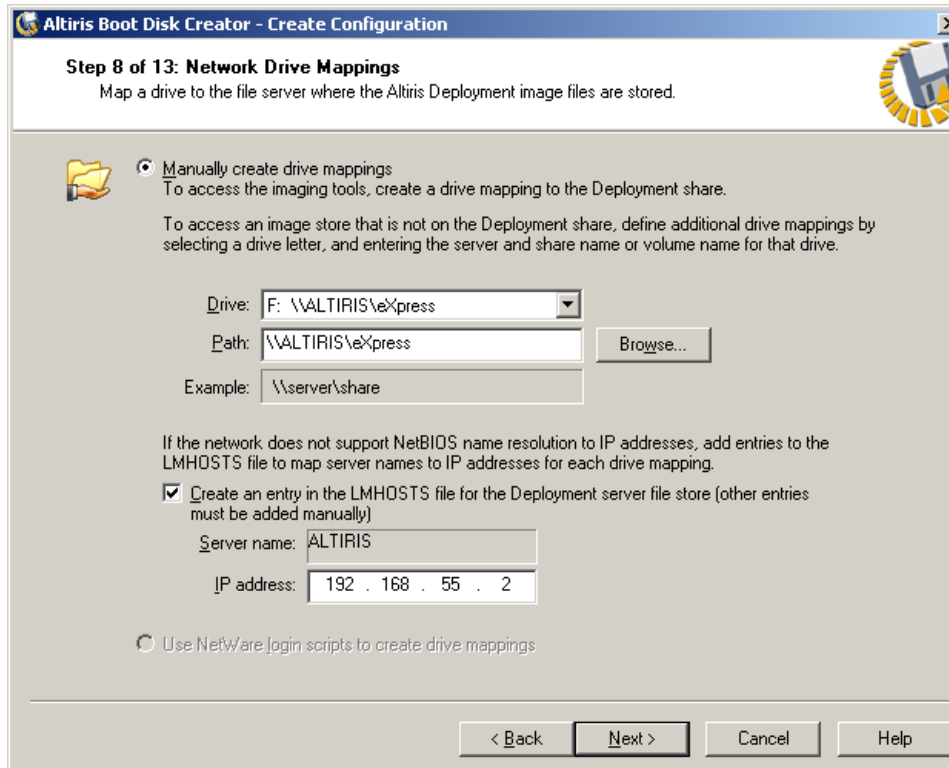


Figure 6-46 The Network Drive Mappings window of the PXE Boot Disk Creator

10. Click **Next** to bypass the Configuration Summary window. This will return you to the window shown in Figure 6-12 on page 185.
11. Click **Next** to move to the next window.
12. Click **Next** to accept the defaults and bypass the Create PXE Boot Image Files window.
13. Click **Finish** to close the Altiris Boot Disk Creator. This will return you to the window shown in Figure 6-11 on page 184. Click **OK** to close the Edit Shared Menu Option window. This will return you to the PXE Configuration Utility. Notice that the Save button is enabled after the boot image has been changed. Click **Save** to save the altered boot image.
14. Click **Save** on the PXE Configuration Utility - Shared Configuration window to save the PXE boot disk image. See Figure 6-17 on page 190.

Important: Make sure to click **Save** when you have finished altering the boot image. If you do not click Save, your changes will be discarded.

Your Windows PE PXE boot image is now ready for use. When you create new jobs (or alter existing jobs) you can now select Windows PE as an automation option. Keep in mind that some jobs such as RAID/Fibre configuring, BIOS updating, and CMOS capturing/deploying require DOS.

Note: It is a best practice to use Windows PE as the PXE boot disk image when doing imaging jobs. Imaging using Windows PE can be up to ten times faster than when using DOS as the pre-boot automation.

Adding mass storage drivers for Windows PE

If Windows PE is being used as your PXE boot disk image and is not able to access the target computer(s) hard disk drives you may need to add the correct mass storage device drivers to the boot image.

To add mass storage device drivers to the Windows PE PXE boot disk image follow the steps outlined below:

1. Open the Deployment Console.
2. Click **Tools** → **Boot Disk Creator** to open the Boot Disk Creator Wizard. If the Boot Disk Creator Wizard splash window appears select **Go to the Boot Disk Creator interface** and then click **OK**.
3. Right-click the **Windows PE Additional Files** folder and select **New** → **Folder** from the pop-up menu.
4. Name the new folder **i386**. Right-click the **i386** folder and repeat the previous step creating a folder named **system32**. Repeat the process and create a folder named **diskdrivers** within the **system32** folder. Your path should look like the figure below.

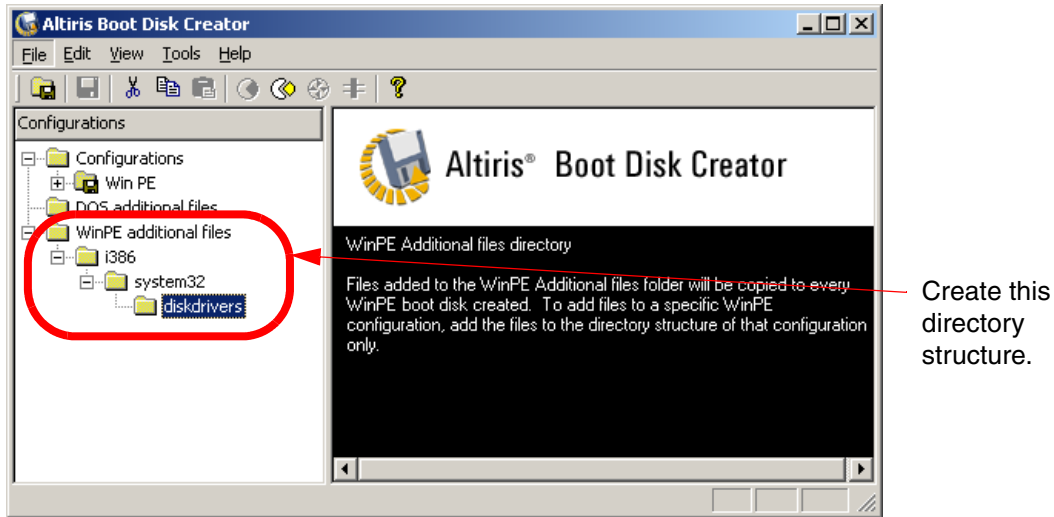
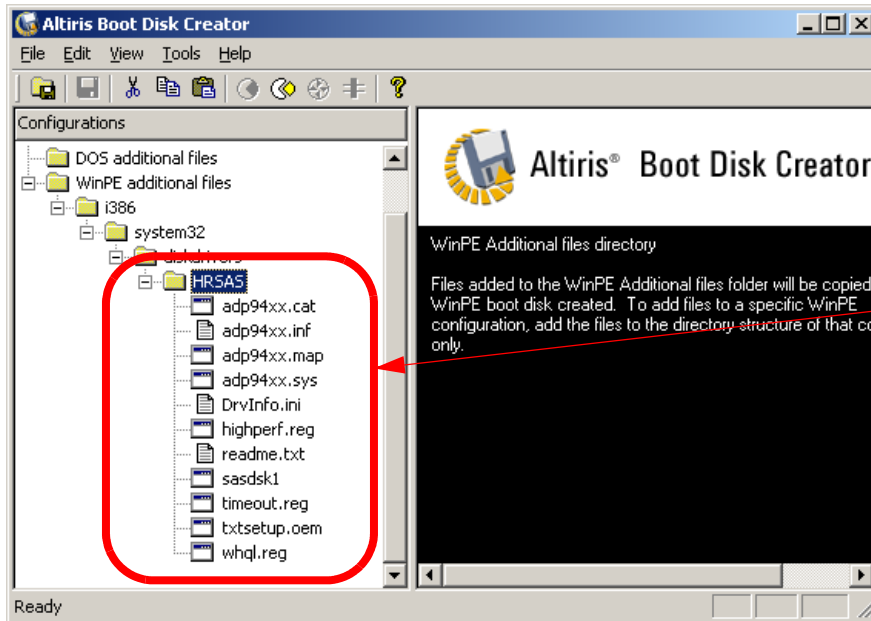


Figure 6-47 The Boot Disk Creator Wizard showing the path for additional mass storage drivers

5. Within the diskdrivers folder, create the folders to contain your drivers. The folders you add should contain a txtsetup.oem file, and at least one *.sys file, and possibly additional files. You must also ensure that any sub-folders specified by txtsetup.oem are included, and that the [defaults] section references the proper device driver (some textsetup.oem files might support multiple devices and drivers, and the proper device must be specified in the [defaults] section).
6. To add the files, right-click the folder you created for the mass storage device drivers and select **Add File** from the pop-up menu. Use the file browser dialog to locate the device drivers you want to add. Select the files and click **Open**. In this example we added the hrsas folder from the ServerGuide CD.



The added mass storage device drivers.

Figure 6-48 The Boot Disk Creator Wizard showing Host RAID SAS drivers added to the image



Post operating system application installation

Altiris Deployment Solution offers the ability to deploy post operating system applications. Applications such as large enterprise management software or even small program updates and hotfixes.

In this chapter we explore some of the various applications that can be deployed as well as the powerful Wise Packager program that comes bundled with Altiris Deployment Solution.

In this chapter we cover the following subjects:

- ▶ 7.1, “Application deployment” on page 230
- ▶ 7.2, “Package deployment” on page 239
- ▶ 7.3, “Using Wise Packager for Deployment Solution” on page 242

7.1 Application deployment

Consider the requirement of deploying 250 new IBM BladeCenter HS20s that are currently sitting on your loading dock still in their original packaging. Your manager wants them up and running with an operating system and all the required applications by Friday at 5:00 PM. It is now 8:15 AM that same day. With the ability to deploy operating system images and your applications configured for automated deployment this scenario is not as impossible as it seems.

The benefits of application deployment can include:

- ▶ Accelerated application deployment

Using a deployment job to distribute post-OS applications to your computers, can make the above scenario possible.

- ▶ Increased productivity

Both your IT staff and end users benefit from application deployment. Not only does your IT staff require less time to install applications, but the end users are faced with a much shorter wait time before using them.

- ▶ Reduced maintenance time and requirements

Using Altiris Deployment Solution to deploy your operating system or application updates and hotfixes helps reduce the time and effort often required to keep a secure and up-to-date infrastructure.

- ▶ Simplified administration

Using deployment jobs to distribute applications means user intervention is out of the picture. Every install uses the same exact settings.

Administration is further simplified by allowing post-OS application deployment to be managed from one single control point, the Deployment Console.

This chapter covers various application deployment sceneries. Based on the examples shown here, you should be able to create your own custom application deployment jobs.

7.1.1 Deploying IBM Director Agent 5.10

Note: This section describes the use of ServerGuide Scripting Toolkit 1.3.02 and IBM Director Agent 5.10.

When the ServerGuide Scripting Toolkit is integrated with Altiris Deployment Solution it provides a default job to deploy the IBM Director Agent. This job will

be used as a the template for creating custom jobs to deploy many other applications.

In this section we dissect the IBM Director Agent deployment job and determine how it will be used for creating custom application deployment jobs. We also cover the deployment of IBM Director Agent to target computers.

The **IBM Director Agent for Windows Install** job can be found in the Jobs pane of the Deployment Console in folder **IBM ServerGuide Scripting Toolkit - version (date) → IBM BladeCenter / xSeries / eServer Support → Applications (Post-OS Installs)**, where *version* is the current version number of the SGTK and *date* is the date it was released to the IBM Web site.

The job as well as the tasks that make-up the job is shown in Figure 7-1.

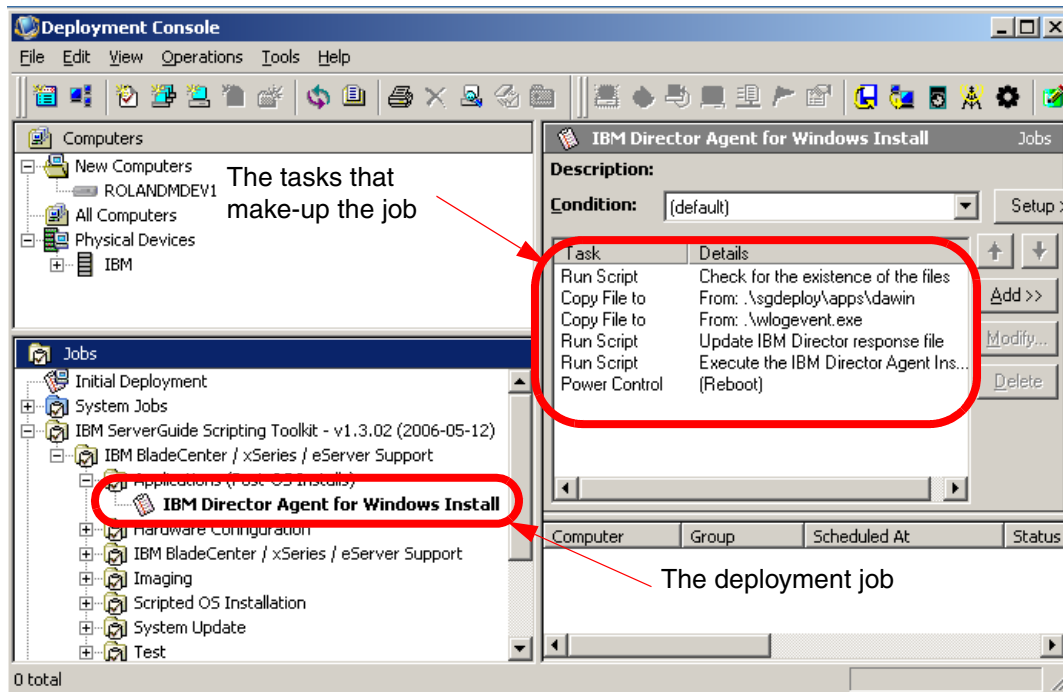


Figure 7-1 The Deployment Console with the IBM Director Agent for Windows Install job

Taking a cursory glance at the tasks that make up the deployment job you can see the basic flow of the script is to:

1. Check for the existence of the required files (installation media) in the Deployment Share.
2. Copy files to the target computer.

3. Update a response file for the IBM Director Agent installer to use.
4. Execute the install process.
5. Reboot the target computer.

This basic flow will be repeated when creating custom jobs to deploy your applications.

In the following sub-sections we will take a closer look at the tasks that make-up the IBM Director Agent for Windows Install job.

Examining the tasks

Open the first task, **Check for the existence of the files**, in edit mode by selecting the task and clicking **Modify**. The task's script is shown in Figure 7-2.

```
REM Check for the existence of the files

if not exist .\sgdeploy\apps\dawin\files\diragent.rsp goto ERR_DA
goto END

:ERR_DA
.\Wlogevent.exe -c:251 -id:%ID% -l:3 -ss:"Can not find the appropriate
application files."

:END
```

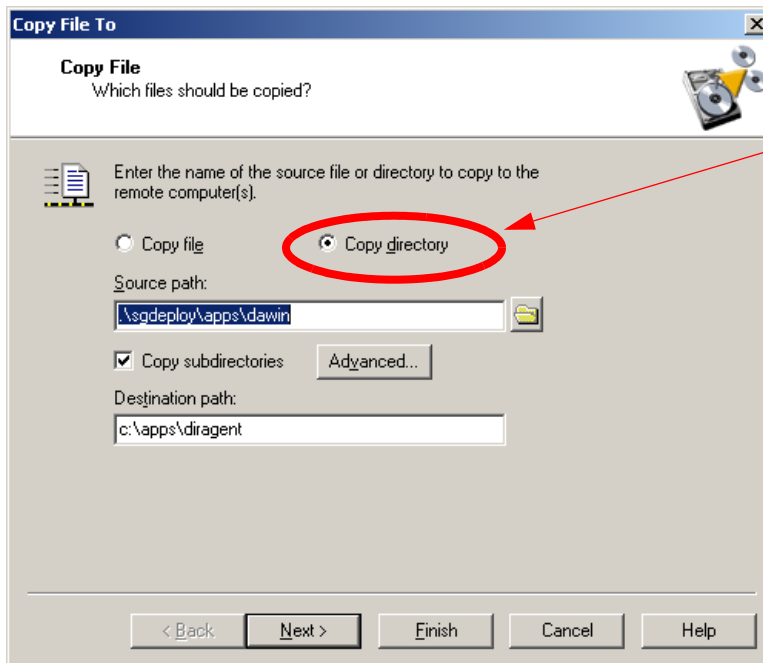
Figure 7-2 The contents of the Check for the existence of the files task

The second line of code looks for a file, named `diragent.rsp`, in the `sgdeploy\apps\dawin` directory. The task is actually looking for the IBM Director Agent installation files in this directory. It makes an assumption that if the `diragent.rsp` file exists in this directory, then the other files required for installation are there also. If the file does not exist the script jumps down to the `ERR_DA` section which logs an event and then ends the script execution which also ends the deployment job. If the `diragent.rsp` file is found execution continues to the next task.

Open the second task, **From: .\sgdeploy\apps\diragent**, in edit mode by selecting the task and clicking **Modify**.

This task looks different than the other tasks we have edited throughout this redbook. This task is a Copy To task type rather than a Run Script task type. Its purpose is to copy either a file or a directory from one location to another.

This particular task is copying the sgdeploy\apps\dawin directory from the Deployment Share to the target computer. The task window is shown below in Figure 7-3.



Copies the entire directory rather than just a file

Figure 7-3 The task window for the Copy To .\sgdeploy\apps\diragent task

Notice that **Copy Directory** is selected. This same type of task can be used to copy either an individual file or an entire directory structure. Also notice that the **Copy Subdirectories** check box is selected. This is to ensure that the contents of any subdirectories are also copied over.

The Source path and the Destination path refer to the location of the installation files and where to save the files on the target computers respectively.

By default, files are copied from the source to the Deployment Server and then to the destination. If you want to copy directly from the source to the destination, click **Advanced** and select **Copy directly from file source**. The three text boxes below will become enabled. Enter a user name with administrative privileges on the computer that has the source files and enter a password for the user. When you are finished click **OK** to return to the task window.

When you have finished examining the task window click **Finish** to save your changes, or **Cancel** to quit without saving.

The next few tasks copy some individual files used by the job's tasks. These files are specific to the IBM Director Agent install and will not be covered in detail. However, one file that is copied is worth mention and can be quite useful when creating your custom jobs. The wlogevent.exe application is used by Altiris Deployment Solution to send the error status back to the Deployment Server. For example, if the first task failed to locate the diragent.rsp file it makes a call to the WLogEvent.exe which notifies the Deployment Server that the task did not complete successfully.

For more information about using the wlogevent.exe application, refer to the *Altiris Deployment Solution 6.5 Reference Guide*, available from:

<http://www.altiris.com/Support/Documentation.aspx>

Open the fifth task, **Execute the IBM Director Agent Installation**, in edit mode by selecting the task and clicking **Modify**. The task's script is shown in Figure 7-4:

```
REM Execute the IBM Director Agent Installation

cd c:\apps\diragent
call diragent.bat
```

Figure 7-4 The task window for the Execute the IBM Director Agent Installation task

This task runs the diragent.bat file on the target computer. The diragent.bat file starts the installation of the IBM director Agent.

The final task, **(Reboot)**, reboots the target computer.

Using the tasks in the IBM Director Agent for Windows Install job as templates, we can create custom jobs to deploy a myriad of other applications.

Deploying IBM Director Agent

Now that you know what the IBM Director Agent for Windows install job is doing, let's go through the entire process of deploying IBM Director Agent from start to finish.

As we discussed earlier, the first task in the job looks for the IBM Director Agent response file, diragent.rsp. If you open the SGTK source tree by clicking **Tools** → **IBM Tools** and then selecting **IBM ServerGuide Scripting Toolkit directory** from the menu and browse to the dawin folder (sgdeploy\apps\dawin\), you will see the folder is empty. The IBM Director Agent files must be copied to the directory before deploying to target computers.

Note: The IBM ServerGuide Scripting Toolkit V1.3.02 supports only Director Agent 5.1 and later.

Complete one of the following procedures to add the IBM Director Agent installation files to the ServerGuide Scripting Toolkit source tree:

Note: The IBM Toolkit Configuration Utility has the ability to import the IBM Director Agent files. See “Add application files” on page 36 for more information.

If you have a copy of the IBM Director Setup and Installation CD, copy the contents of the \director\agent\windows\i386 folder on the CD into the sgdeploy\apps\dawin folder in the source tree.

Or:

If you are getting the Director Agent installation files from the IBM Web site, complete the following steps:

1. Locate and download the IBM Director Agent installation ZIP file (dir5.10_agent_windows.zip for IBM Director Agent 5.10) from the IBM Web site.
2. Extract the IBM Director Agent installation files from the ZIP file into the sgdeploy\apps\dawin directory in the SGTK source tree.
3. In the sgdeploy\apps\dawin folder in the SGTK source tree, rename the installation executable file (for example, IBMDirectorAgent5.10.exe) to IBMDir~1.exe.
4. In the sgdeploy\apps\dawin folder in the SGTK source tree, rename the diragent_windows.xml file to dirage~1.

Once you have copied the IBM Director Agent installation files to the SGTK source tree, you can deploy the IBM Director Agent for Windows Install job by drag-and-dropping the job onto any active computer or group of computers in the Computers pane of the Deployment Console.

7.1.2 Deploying Microsoft SQL Server 2000 (case study)

Before deploying Microsoft SQL Server 2000 using Altiris Deployment Solution, some setup must be performed.

The follow bulleted list summarizes the steps that must be performed before deploying:

1. Copy the installation media to the SGTK source tree
2. Customize a response file
3. Customize a deployment job with the script and imaging tasks

This section will cover the items listed above.

Copy the installation media to the Deployment Share

Before creating a customized job to deploy SQL Server 2000, the installation files need to be copied to the ServerGuide Scripting Toolkit source tree.

Follow the steps below to copy the installation media:

1. Insert the installation media for SQL Server 2000 into the CD-ROM drive.
2. Using Windows Explorer open the CD and copy the entire contents to directory “.\sgdeploy\apps\SQL2000”.

Note: By default the SQL2000 directory does not exist and will need to be created.

Customize a response file

After the installation media has finished copying, open the SQL2000 directory you just created and browse the files. In the root directory, SQL Server has a number of files with the ISS extension. These are response files for unattended installation. By default, the *SQL 2000 Unattended Install job uses the SQLINS.ISS response file. However, if you want to create your own response file, copy the SQLINS.ISS to use as a template and edit the duplicate file to meet your needs. Once you have made your changes, save the response file with a different name than the original.

For detailed information about altering SQL Server 2000 response files visit the Microsoft Web site at the following URL:

<http://support.microsoft.com/default.aspx?scid=KB;en-us;q233312>

Customize a deployment job with the script and imaging tasks

Altiris Deployment Solution comes with a sample job for deploying SQL Server 2000. The sample jobs that come with Altiris Deployment Solution are located in the Samples container in the Jobs pane of the Deployment Console.

The ***SQL 2000 Unattended Install** job is located in folder “Samples\Server Applications\SQL 2000”.

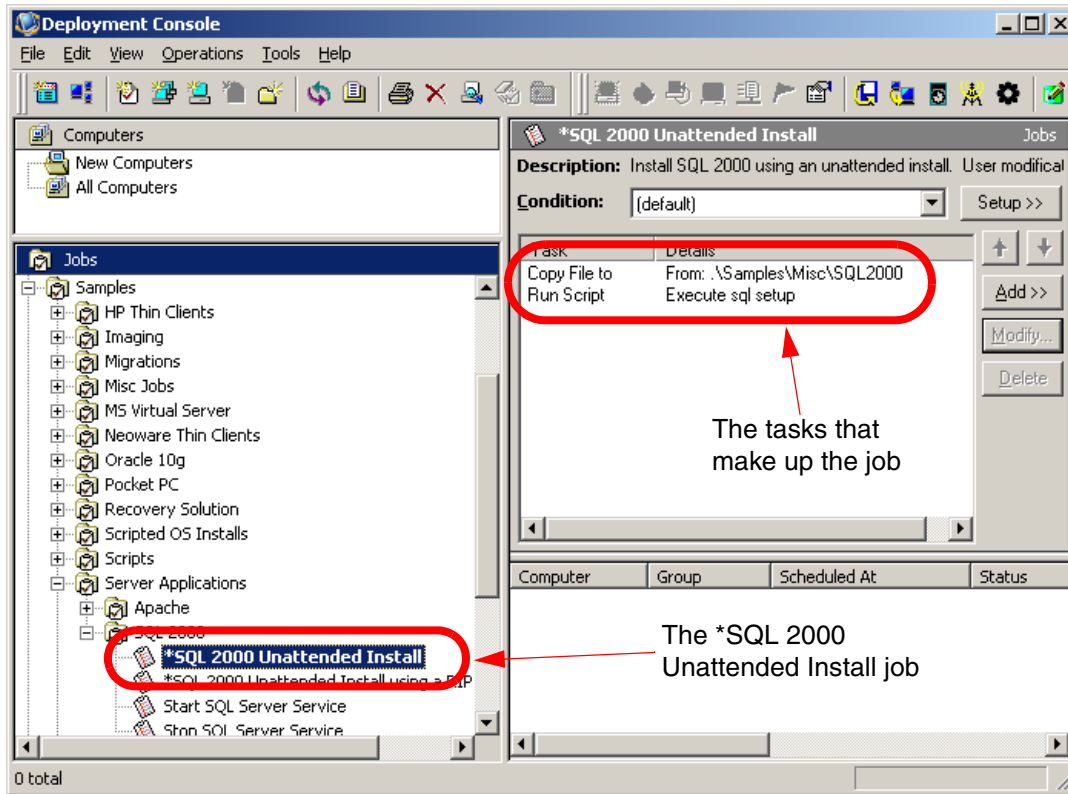


Figure 7-5 The Deployment Console with the *SQL 2000 Unattended Install job highlighted

This sample job can be used as a template for creating your own custom job for installing Microsoft SQL Server 2000.

To create your own custom job for installing SQL Server 2000 follow the steps below:

1. Right-click the ***SQL 2000 Unattended Install** job and select **Copy** from the pop-up menu.
2. Right-click elsewhere in the Jobs pane and select **Paste** from the pop-up menu. This creates a duplicate of the original job. We will make changes to the duplicate so the original is not overwritten.
3. Click on the duplicate *SQL 2000 Unattended Install job you created in step 2. In the Details pane of the Deployment Console select the first task and click **Modify**.
4. Replace the path to the SGK source directory with `.\sgdeploy\apps\sql2000` and click **Finish** to exit the task editor window.

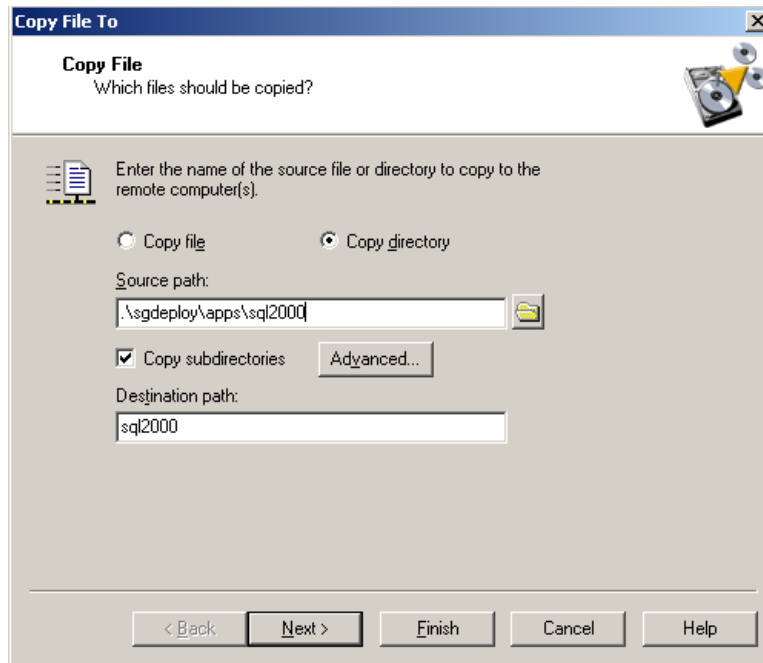


Figure 7-6 The Copy File To task of the *SQL 2000 Unattended Install job after changes

5. If you decided to create your own custom SQL Server 2000 response file, the second task of the *SQL 2000 Unattended Install job will also need to be altered. In the Details pane of the Deployment Console select the second task, labeled **Execute sql setup**, and click **Modify**. Figure 7-7 shows the task script.

```
REM Execute sql setup
start /wait sql2000\x86\setup\setupsql.exe -s -m -SMS -f1
"sql2000\sqlins.iss"
```

Figure 7-7 The Execute sql setup task of the *SQL 2000 Unattended Install job

Change the portion “sql2000\sqlins.iss” to the name of your custom response file. For example, if you created a custom response file named mysqlrsp.iss then you would change that portion to “sql2000\mysqlrsp.iss”.

6. Click **Finish** when you are done making changes to exit the task editor window.

Your custom SQL Server 2000 installation job is ready for deployment. You can deploy it by drag-and-dropping the job onto any active computer or group of computers in the Computers pane of the Deployment Console.

7.2 Package deployment

Package deployment allows you to deploy small applications, such as hotfixes, patches, or updates. The basic premise is anything that does not require a response file and can be run silently (without user intervention) is an excellent candidate for package deployment.

Before deploying a simple application using Altiris Deployment Solution, some setup must be performed:

- ▶ Copy the installer package to the deploy directory in the Deployment Share
- ▶ Customize a deployment job to deploy the package

This section will cover the items listed above.

7.2.1 Install a Microsoft Windows hotfix package

To demonstrate the abilities of package deployment we will create a custom deployment job to deploy a Microsoft Windows hotfix package.

Copy the installation media to the Deployment Share

Before creating a customized job to deploy a Microsoft Windows hotfix package, the actual update executable needs to be copied to the deploy directory in the Deployment Share.

Follow the steps below to copy the installation media:

1. Obtain the Windows hotfix from the Microsoft support site.
2. Copy the update into the Deploy\msupdt directory of the Deployment Share

Note: By default the msupdt directory does not exist and will need to be created.

Customize a custom deployment job

Once you have copied the Microsoft Windows hotfix package into the msupdt directory, you can create a custom deployment job to deploy the package.

Follow the steps below to create a custom deployment job:

1. Open the Deployment Console

2. Right-click an empty area in the Jobs pane and select **New Job** from the pop-up menu. The new job will appear in the Jobs pane.
3. Give the job a name such as **Deploy Windows Update KB835732**.

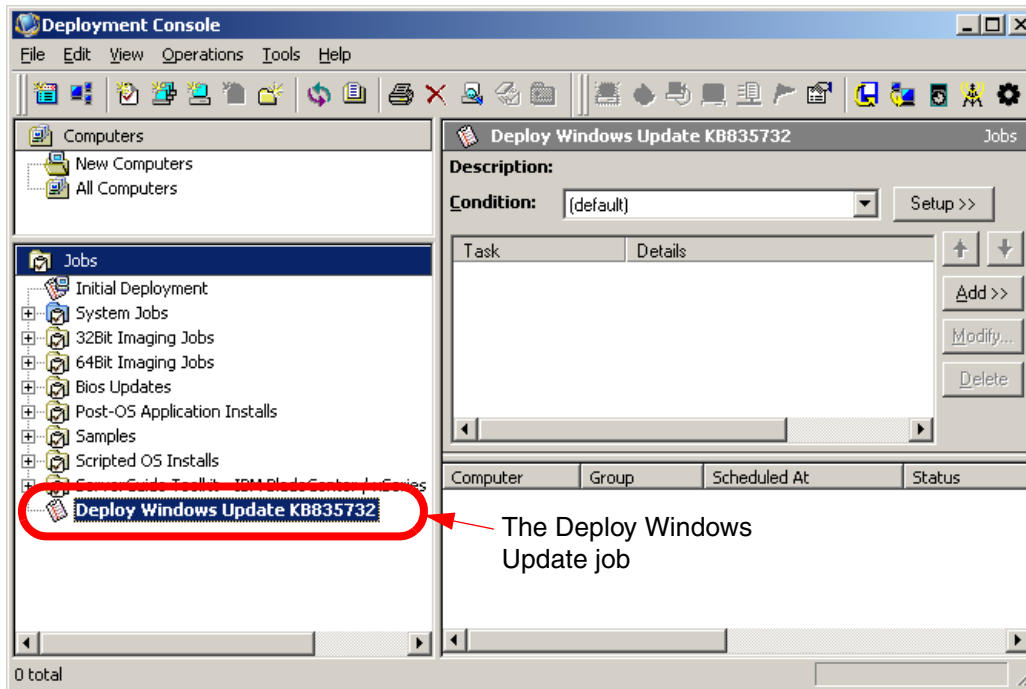


Figure 7-8 The Deployment Console with the new Deploy Windows Update job

4. Notice in the Details pane that no tasks are included in the job. This is a new job that has not been based on a template job, and thus has no tasks included. Click **Add** in the Details pane to add a task. Select **Distribute Software** from the pop-up menu. This will open the Software Package Options window.

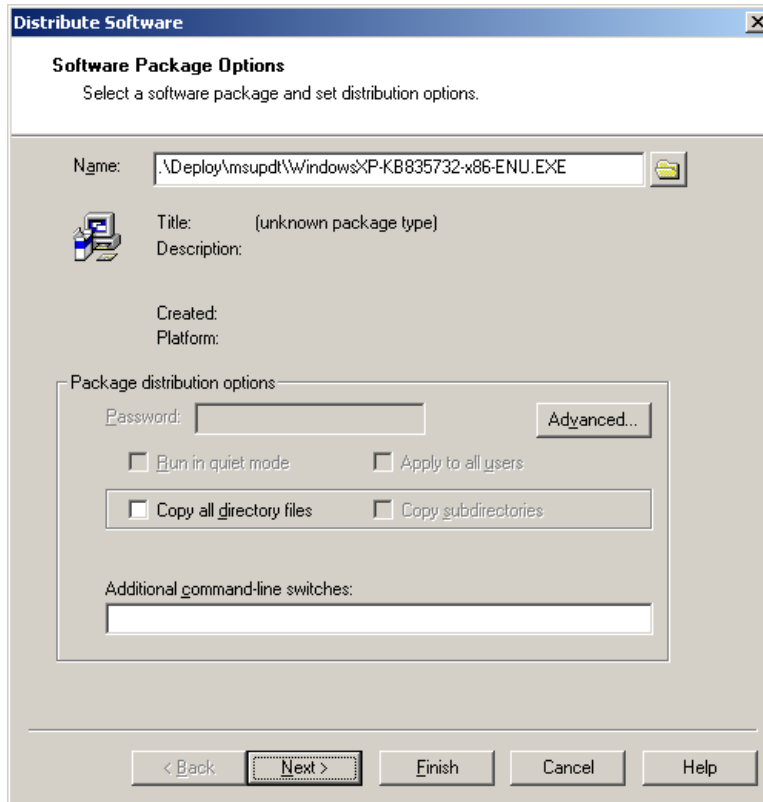


Figure 7-9 The Software Package Options window

5. Click the **Folder** icon and browse to the Deploy\msupdt folder and select the Windows Update package you copied to the folder.
6. If your package supports additional command-line switches such as /q for a quiet install, enter them into the text box labeled **Additional command-line switches**.

Note: If you are deploying an Microsoft Installer package (MSI) the check box labeled **Run in quiet mode** will become enabled. Check this check box to deploy the package silently (without user intervention).

For more information about Microsoft software switches visit the Microsoft Web site at the following URL:

<http://support.microsoft.com/kb/824687>

7. Click **Finish** to complete the creation of your custom deployment job.

Your custom Microsoft Windows Update job is ready for deployment. You can deploy it by drag-and-dropping the job onto any active computer or group of computers in the Computers pane of the Deployment Console.

7.3 Using Wise Packager for Deployment Solution

Ideally, package deployment requires zero user intervention during the install process. As you know, many applications require various settings to be configured during install and do not come equipped with the ability to use response files. Wise Packager is the answer to this problem.

Wise Packager for Altiris Deployment Solution lets you repackage software applications so you can deploy them to end users using Altiris Deployment Solution.

Wise Packager for Altiris Deployment Solution consists of 2 tools:

- ▶ SetupCapture
 - SetupCapture records all the changes performed by an installation and saves that information to a new Windows Installer installation package (MSI file).
- ▶ Wise MSI Editor
 - Wise MSI Editor lets you edit Windows Installer installation packages. You can:
 - Create software installations in an industry standard format (Windows Installer).
 - Make basic changes to simple applications that you are repackaging into Windows Installer format.
 - Create transforms for the applications that you are repackaging.

For detailed information regarding Wise Packager for Altiris Deployment Solution see the WisePackager.chm file in the Wise Packager\Help directory in the Deployment Share.

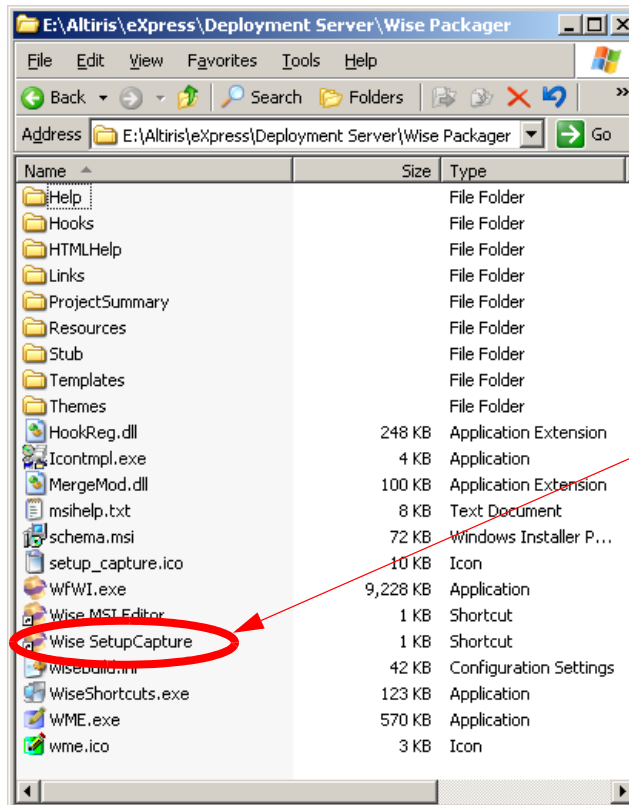
7.3.1 Capturing an application installation

For this example we will be capturing the installation of IBM Director Agent 5.10.

It is a best practice to use a clean computer (one which is running a freshly installed operating system) as the Reference Computer. Before beginning the capture process, close down all applications that may be running on the Reference Computer.

To capture an application install and create a Microsoft Installer package follow the steps outlined below:

1. From the Reference Computer map a drive to the Deployment Share on the Deployment Server.
2. Open the mapped drive and browse to the Wise Packager directory in the Deployment Share
3. Start Wise Packager SetupCapture for Altiris Deployment Solution by clicking the shortcut labeled **Wise SetupCapture**.



Click on the shortcut labeled **Wise SetupCapture** to start the capture process

Figure 7-10 The Wise Packager folder in the Deployment Share

4. On the Specify Target Installation File window, click **Browse** and browse to the location where you want to create your MSI file. Give the MSI file a meaningful name. For this example we named ours **IBMDirectorAgent.msi**.

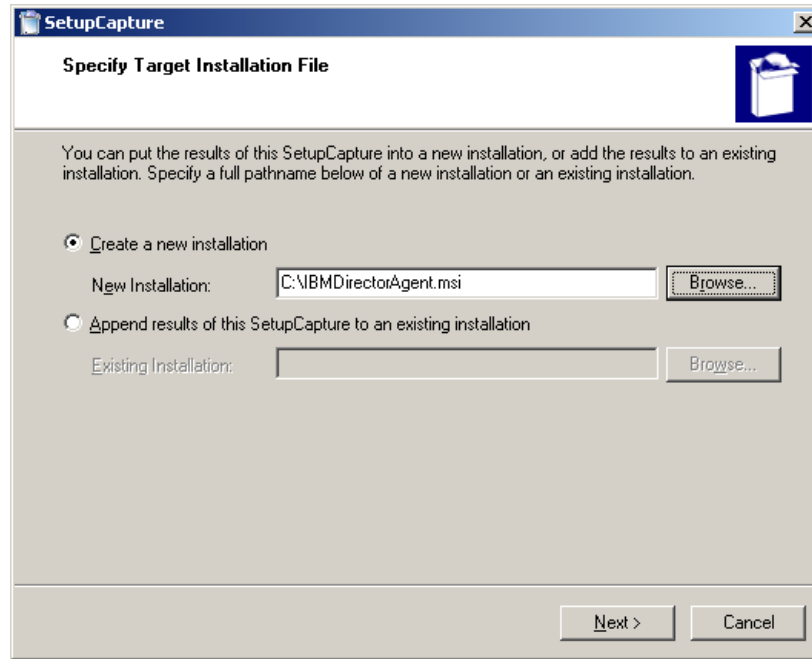


Figure 7-11 The Specify Target Installation File window of SetupCapture

If you are appending results onto an existing MSI file you would have selected **Append results of this SetupCapture to an existing installation** and clicked the lower **Browse** button to browse to the existing MSI file. We are creating a new installation so we chose the top-most radio button. Click **Next** to continue.

5. The Welcome window simply has a button to enter the Settings window. If you want to edit settings such as registry key exclusions, folders to watch, and so forth, click **Settings**. To learn more about the various settings refer to the user manual available from the Help menu of the Wise MSI Editor. We will accept the default settings and click **Next** to continue.
6. The Begin Installation Capture window is simply to remind you to exit all other applications before beginning the capture process. Once you have exited all other applications, click **Next** to continue.

Important: SetupCapture tracks changes to the Reference Computer while the installation is taking place. If other applications are making changes to the Reference Computer those changes will also be recorded. Also, any changes you make to the Reference Computer (such as changing the IP address) during the capture process will be recorded.

- SetupCapture now scans the Reference Computer and the Reference Computer's Windows registry to create a baseline for later comparison. When the scan has finished, the Execute Installation window loads. Click **Browse** to browse to the application's executable that you want to capture. If you want to add any additional command line parameters, enter them into the **Command Line** text box. Click **Execute** to begin installation of the application.

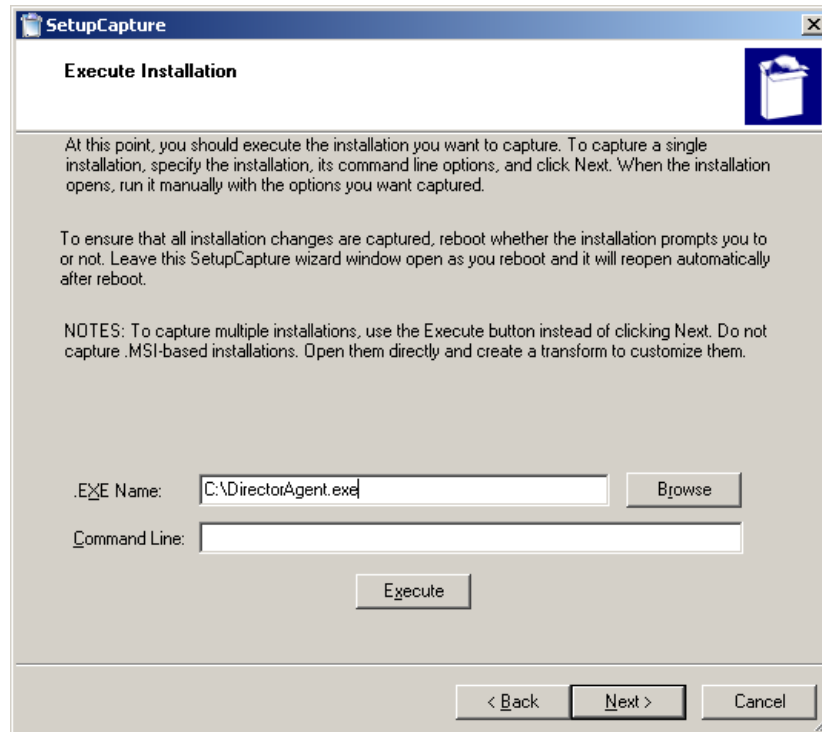


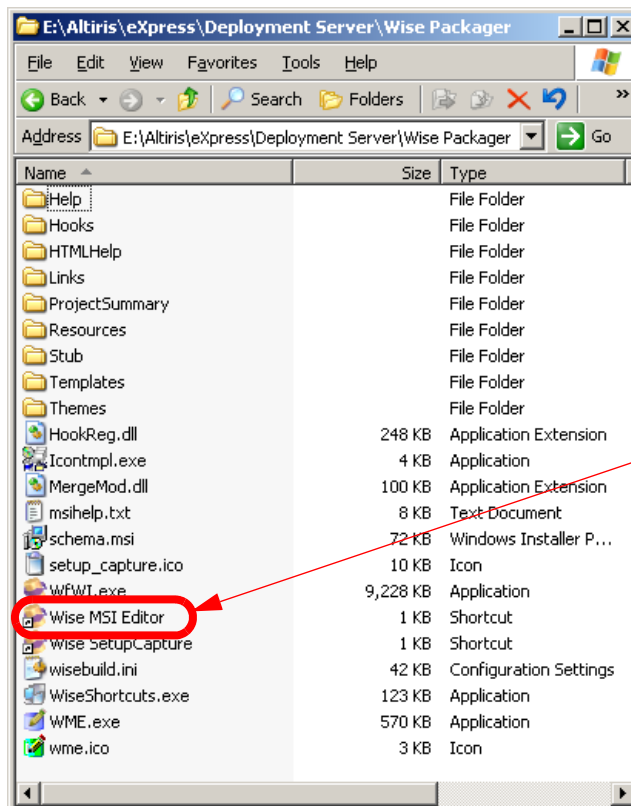
Figure 7-12 The Execute Installation window of SetupCapture

- Proceed through the application's install process as you would normally. Once you have finished the installation, reboot the Reference Computer without exiting SetupCapture. SetupCapture will reload when you boot back into the operating system.

Note: It is possible to include multiple application installs into a single MSI file. To do so, click **Browse** and find your next application's executable file, then click **Execute**.

9. After the Reference Computer reboots and SetupCapture reloads, click **Next** to continue. The End Installation Capture window asks you whether you are sure you are done. If you are finished, click **Next** to continue.
10. SetupCapture builds the MSI file. When it has finished, click **Finished** to exit SetupCapture.

The MSI file is complete and ready to be deployed. However, the MSI file is somewhat “raw.” For example, it will not have a name in Windows Add/Remove Programs. If you want to make further improvements on the MSI file, open the Wise MSI Editor by double-clicking on the shortcut labeled **Wise MSI Editor** in the Wise Packager folder in the Deployment Share as shown in Figure 7-13.



Double-click the shortcut labeled **Wise MSI Editor** to make changes to an existing MSI file

Figure 7-13 The Wise Packager folder in the Deployment Share

To deploy your MSI file follow the steps outline in 7.2.1, “Install a Microsoft Windows hotfix package” on page 239.

7.3.2 Guidelines for using Wise SetupCapture

The following are best practices for using Wise SetupCapture to capture application installs.

- ▶ Run SetupCapture on a clean machine (a fresh operating system installation).
- ▶ Do not run SetupCapture from the Deployment Console; run it from the Reference Computer.
- ▶ During a capture, SetupCapture attempts to convert computer-specific and user-specific data in the registry to generic data that will work on any computer. It does this by searching for standard paths (example: C:\Winnt) and replacing them with Windows Installer properties (example: [WindowsFolder]).

Part of this process includes searching for the computer name and currently logged-on user name. To make the search for computer and user names as accurate as possible, make sure the computer name and user name on the capture computer are set to unique names 4 or more characters in length. Avoid having the user name or computer name set to any common file or folder names. An example of a unique user name is: repack-age-1-user.

- ▶ Before you run SetupCapture, exit all other applications, including background services or applications. (Example: Symantec AntiVirus.)
- ▶ During SetupCapture, changes to an INI file are recorded as “INI file changes” only if the file is in the standard INI file format. Otherwise, the changes are recorded as simple file change.
- ▶ Do not capture an MSI-based installation. Instead, open the MSI directly in Wise MSI Editor. To customize it for specific workgroups, create a transform. See *Creating a Transform Based on an Existing MSI* in the Wise Packager help file. You must be able to run the original installation to repack-age it with SetupCapture. For example: If the installation requires a serial number, you must have the serial number.
- ▶ SetupCapture does not monitor any internal logic within the installation and it does not replicate the user interface of the original installation.
- ▶ SetupCapture creates a separate feature for each EXE that's installed that has a shortcut. Isolating EXE components into features results in more efficient repairs, because if there is a problem with a component, only the problem component and the EXE are reinstalled instead of the entire feature containing the problem component.
- ▶ To capture an uninstall, you must mark **Include files deleted during capture** and **Include registry keys deleted during capture** in SetupCapture Configuration General Settings. In Wise MSI Editor, deleted items are located in the RemoveFile and RemoveRegistry tables in **Setup Editor** → **Tables** tab.

- ▶ Registry keys that define an environment variable are converted to an environment variable in the repackaged installation.



Integrating with IBM Director

IBM Director is a comprehensive utility designed to manage the full IBM Systems product family, including desktop PCs and notebooks. It's a simple, flexible suite of tools for managing systems, maximizing system availability, and lowering IT costs. IT Administrators can use IBM Director to monitor the hardware configuration, usage, and performance of remote systems, including specific components such as processors, disks and memory.

This chapter describes how Altiris Deployment Solution integrates with IBM Director using either upward integration through the Altiris Connector Pack 6.0 for IBM Director or by extension through the Altiris Deployment Server Extension 1.0 for IBM Director.

This chapter covers:

- ▶ 8.1, "How to integrate with IBM Director" on page 250
- ▶ 8.2, "Upward integration" on page 251
- ▶ 8.3, "Integration by extension" on page 289

8.1 How to integrate with IBM Director

Deployment Solution integration with IBM Director can be accomplished in two ways.

The first method is designed to meet the needs of customers with a large investment in Altiris solutions. It requires additional Altiris software such as Notification Server, Connector Solution, and the Connector for IBM Director. This method is viewed as an upward integration module for IBM Director.

For upward integration the following software is required:

- ▶ **Altiris Notification Server 6.0 with Service Pack 3:** This must be installed in the same subnet as the other software components.
- ▶ **Altiris Connector Solution 6.1:** This must be installed on the same computer as Notification Server.
- ▶ **Altiris Connector for IBM Director:** This must be installed on the same computer as Connector Solution. If Connector Solution is not installed, the Connector for IBM Director will install it for you.
- ▶ **Connector Agent for IBM Director:** This must be installed on the IBM Director Server to complete the integration.
- ▶ **IBM Director Server 5.1:** This must be installed and running in the same subnet as the other software components.

The second method is for customers that have a smaller investment in Altiris solutions (most are running only Deployment Solution) but have a strong focus on IBM hardware and IBM Director. This method uses an extension to IBM Director.

For the IBM Director extension the following software is required:

- ▶ **Deployment Server Extension 1.0 for IBM Director:** This is a free install that is available on the Altiris Web site.
- ▶ **IBM Director Server 5.1:** This must be installed and running in the same subnet as the other software components.

Note: The installation of IBM Director is not covered in this document. Please reference the documentation on the IBM Director installation CD or the IBM Redbook *Implementing IBM Director 5.10*, SG24-6188.

In this chapter, we cover both methods:

- ▶ 8.2, “Upward integration” on page 251
- ▶ 8.3, “Integration by extension” on page 289

8.2 Upward integration

Upward integration is the best solution for customers that have a large investment in Altiris solutions. Most customers that fit into this category will already have the required software (such as Notification Server and Connector Solution) installed. Upward integration provides these customers with the ability to access more IBM specific information for reporting and the ability to share data between IBM Director and the Notification Server

For the sake of completeness, this chapter covers the install and basic configuration of Notification Server and Connector Solution before covering the upward integration module (Altiris Connector for IBM Director).

8.2.1 Altiris Notification Server 6.0 with Service Pack 3

Notification Server is a product used to support Altiris solutions such as Deployment Solution. Altiris Notification Server provides the core functionality used by Altiris solutions, such as security, reporting, console interface, and communications with other computers. An Altiris solution plugs into Notification Server to leverage Notification Server's functionality.

With Notification Server you can deploy programs and run them on a scheduled basis. You can gather inventory information about your client computer's hardware, software, and more and then save the information in a database (the Notification Database). You can also push the Altiris Client software from the Notification Server to the client computers.

Note: The Altiris Agent is not the same agent software as the Deployment Agent.

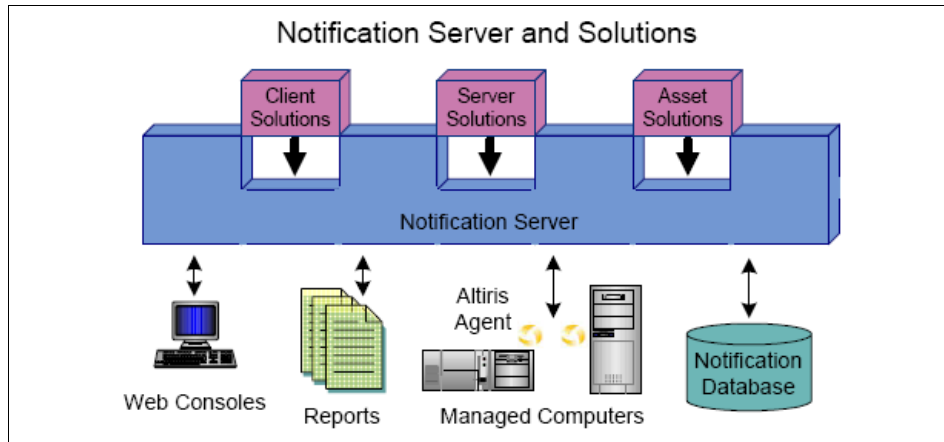


Figure 8-1 Notification Server and Solutions

Notification Server lets administrators move from the role of doing tasks to the role of defining policies that automate tasks. Notification Server runs based on policies defined by an administrator. These policies activate components of Notification Server that are used to process and store inventory data, host Web pages, forward data to SMS, and many other tasks. This simplifies the administration of computer management in your distributed network environment.

Notification Server policies run on the server in the context of Microsoft Component Services. Notification Server automatically distributes the conditions to be monitored on the NS Clients, and when a specific condition is found, the Notification Server is notified. It then runs a script that executes the instructions that have been specified by the administrator.

Reports can be viewed from a Web browser-based Altiris Console (Web Administration Console) or from any browser in the network. The reports provided with Notification Server give summary level details with the ability to interactively drill down for additional detail.

For those using Microsoft Systems Management Server (SMS), Notification Server can be viewed as a companion product for the SMS Site Server. Notification Server extends the reach of SMS by providing seamless integration for UNIX systems and remote/mobile users, as well as standalone environments. Notification Server extends the functions of SMS by providing support for Active Management solutions that enable real-time detection, and notification of problems.

Notification Server components

Notification Server consists of many components; the primary ones are:

- ▶ **Notification Server:** provides services to solutions, processes events, manages data, runs tasks, runs reports, and enforces security settings.
- ▶ **Notification Database:** Stores data collected by Notification Server and solutions.
- ▶ **Altiris Agent:** Installed on computers to facilitate interactions between Notification Server and the managed computer (a computer with the Altiris Agent installed and managed by Notification Server). The agent receives configuration information from and sends data to Notification Server. The agent also helps in downloading files and installing and managing solution-specific agents.
- ▶ **Reports:** Specially organized views of data. Data can be organized into lists, tables, or graphs.
- ▶ **Web-based management consoles:** Interfaces between the user and Notification Server and solutions.

Hardware requirements for Notification Server

The following are minimum hardware requirements for Notification Server. To scale to support thousands of clients, faster processors and more memory are highly recommended on the server.

- ▶ Processor: Pentium® III 800 MHz or faster
- ▶ RAM: 512 MB (1 GB is recommended)
- ▶ File System: NTFS partition
- ▶ Disk space: 2 GB (20 GB recommended)

Software requirements for Notification Server

The following are minimum software requirements for Notification Server.

Note: The Install Helper (covered in more detail in “Installing Notification Server 6.0 with Service Pack 3” on page 254) determines whether the computer has the necessary prerequisite software installed, and if software is missing it will help you download and install the needed software.

- ▶ Operating system (one of the following):
 - Recommended: Windows 2003 SP1 or
 - Approved: Windows 2000 Server or Advanced Server with SP3.
- ▶ SQL Database (one of the following):
 - Recommended: Microsoft SQL Server 2000 SP3.

- Approved: MSDE. If you don't have a SQL Server, Install Helper will help you install MSDE 2000
- ▶ Web server:
 - Microsoft Windows Internet Information Services (IIS) (this component is not installed by default with Windows 2000 and above).
- ▶ Services:
 - Microsoft .NET 1.1 Framework (with ASP .NET) or later and Microsoft Data Access Control 2.7
- ▶ Web Browser:
 - Microsoft Internet Explorer® 6.0 or later

Note: This document assumes a working knowledge of Notification Server 6.0. For more information about Notification Server, reference the *Altiris Notification Server 6.0 SP3 Reference Guide* available from:

http://www.altiris.com/upload/notificationref_001.pdf

Installing Notification Server 6.0 with Service Pack 3

If Notification Server is not installed in your environment it can be installed automatically when you install any Notification Server based solutions (such as Connector Solution or the Connector for IBM Director). The benefit to this approach is that each Notification Server based solution comes with an Install Helper tool that examines the computer on which you are installing Notification Server to verify it meets the requirements.

For this example we will download the Connector for IBM Director and use the Install Helper to kick-off the installation of Notification Server. If you want to access the Notification Server install package directly it can be found at the following URL:

http://www.solutionsam.com/solutions/6_0/Altiris_NS_6_0.exe

Note: Connector for IBM Director is covered in greater depth in 8.2.3, “Altiris Connector for IBM Director” on page 267.

Download the Connector for IBM Director install package from the following URL:

<http://www.altiris.com/Products/ConnectorforIBMDirector.aspx>

Save the package on the computer you want to use as the Notification Server.

Once you have downloaded and extracted the zipped package, follow the steps below to run the Install Helper and to kick off the install of Notification Server:

1. Using Windows Explorer browse to the folder where you extracted the Connector for IBM Director package. Run the Install Helper by double-clicking the file named **NSInstallHelper.exe**.

This tool will determine if the computer you want to use as the Notification Server meets all the hardware and software requirements. If the computer does not meet the prerequisites the Install Helper will give you instructions on how to meet the requirements.

2. When the first window loads, click **Next** to begin the prerequisite check.
3. On the second window you are asked if you are installing Notification Server on the local computer. Because we saved the package on the computer we are using as the Notification Server, we select **Yes**. Click **Next** to continue.

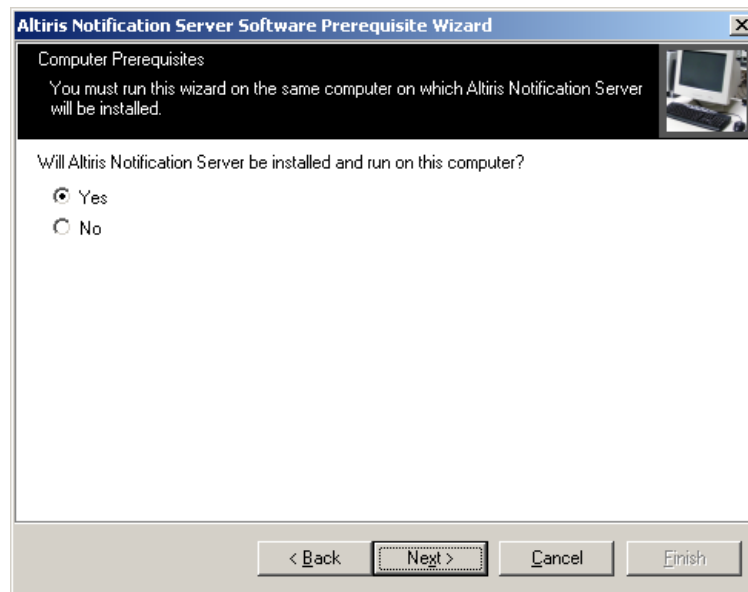


Figure 8-2 Select Yes to check the local machine

4. The Install Helper will check the local computer so see if it meets the requirements. If a requirement is not met, the missing item will be displayed in the window. To view information about how to satisfy the requirement, double-click the missing item.

Once you have met all the requirements, click **Next** to continue.

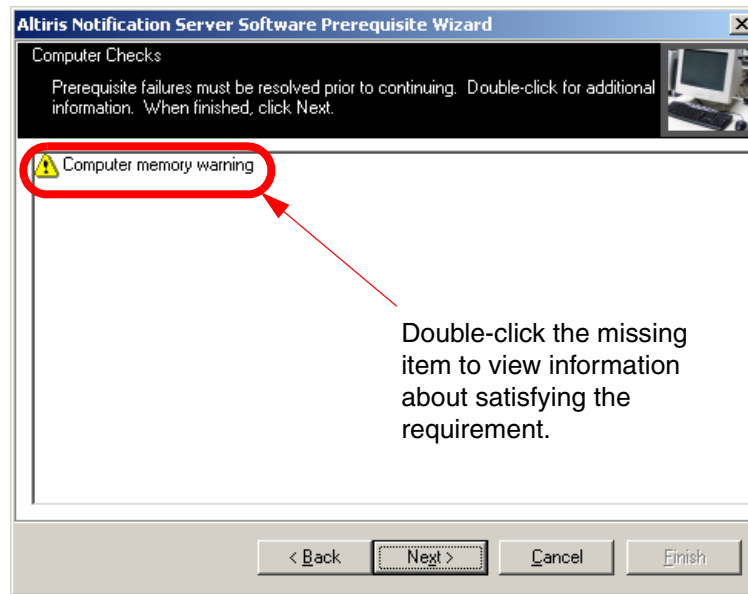


Figure 8-3 Double-click the missing item to view information about how to satisfy the requirement

5. Once all the requirements have been met, the final window appears and lists the URL for the Notification Server download. Click **Finish** to close the Install Helper and open a Web browser to the URL.
6. If you are asked to Open or Save the Altiris_NS_6_0.exe file, select **Save**. Save the file on the computer you want to use as the Notification Server.
7. Browse to the Notification Server executable file and launch the install by double-clicking the Altiris_NS_6_0.exe file. The executable will extract the files necessary for the install and launch the InstallShield Wizard. Click **Next** to begin the install.
8. To accept the licensing agreement, select **I accept the terms in the license agreement** and click **Next**.
9. On the Customer Information window enter a user name and an organization name. This is generic information and can be any text string you want to use. Click **Next** to continue.

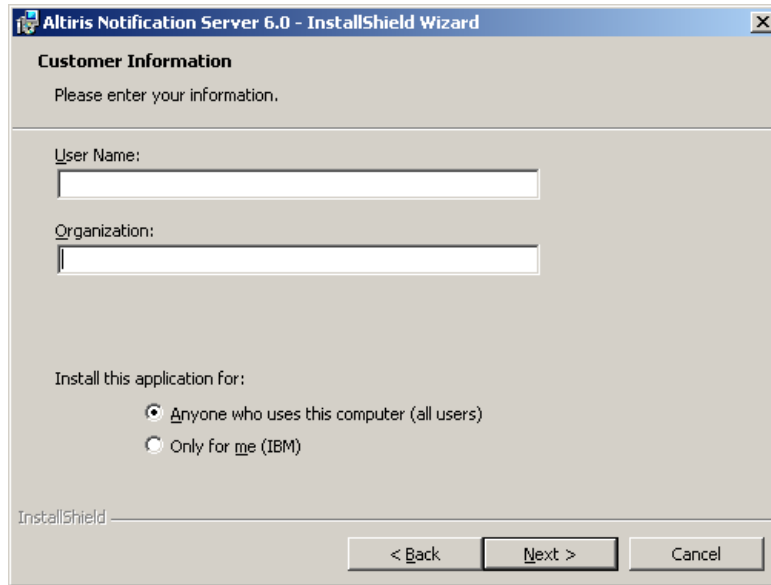


Figure 8-4 The Customer Information window of the install process

10. On the Setup Type window verify that **Complete** is selected and click **Next** to continue.
11. Click **Install** to install Notification Server.
12. After the InstallShield Wizard copies the files click **Finish** to close the InstallShield Wizard.

Configuring Notification Server

After Notification Server has been installed, a series of configuration pages open automatically. To configure Notification Server follow the steps outlined below:

1. On the User Identity Settings page of the Notification Server configuration process, enter a user name with local administrative privileges in the text box labeled **User (domain\user)**. In the text box labeled **Password**, type the password for the user account entered above. Click **Next** to continue.

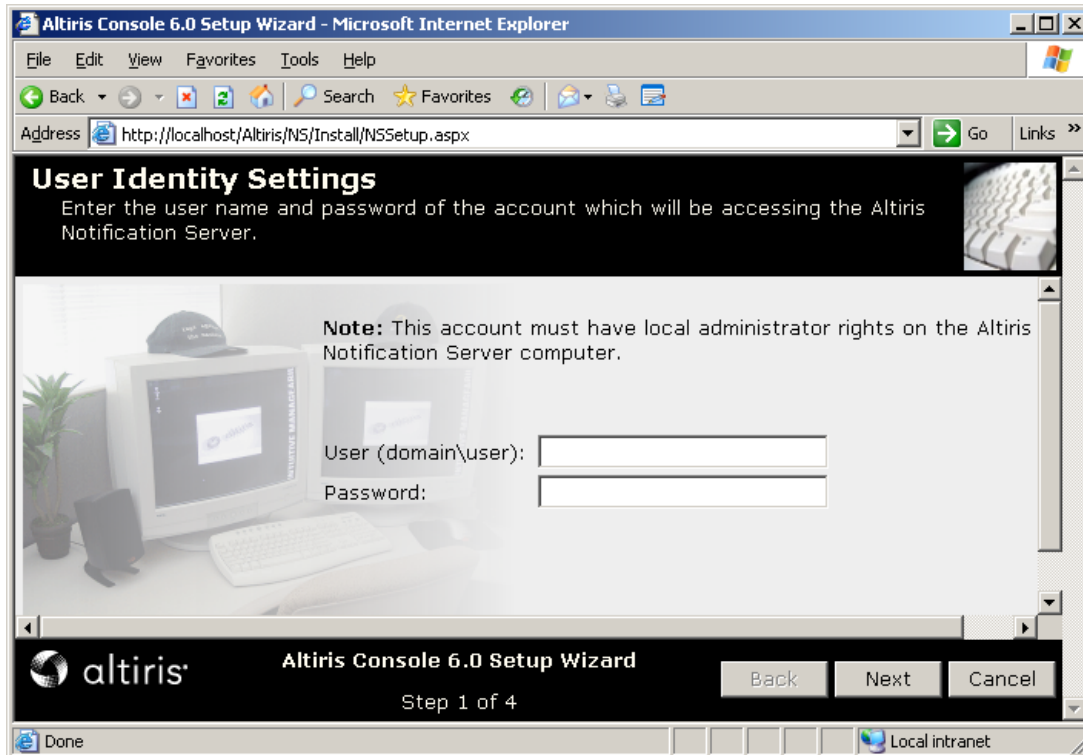


Figure 8-5 The User Identity Settings page of the Notification Server configuration process

2. The E-mail Settings page lets you set up an e-mail address that will receive administrator alerts from Notification Server when system events are generated. Enter the DNS name or IP address of your SMTP server. You must also enter a valid user name and password to log on to the SMTP server if the server requires authentication. Click **Send Test E-mail** to send a test e-mail and verify that Notification Server is sending e-mail to the correct address. Click **Next** to continue.

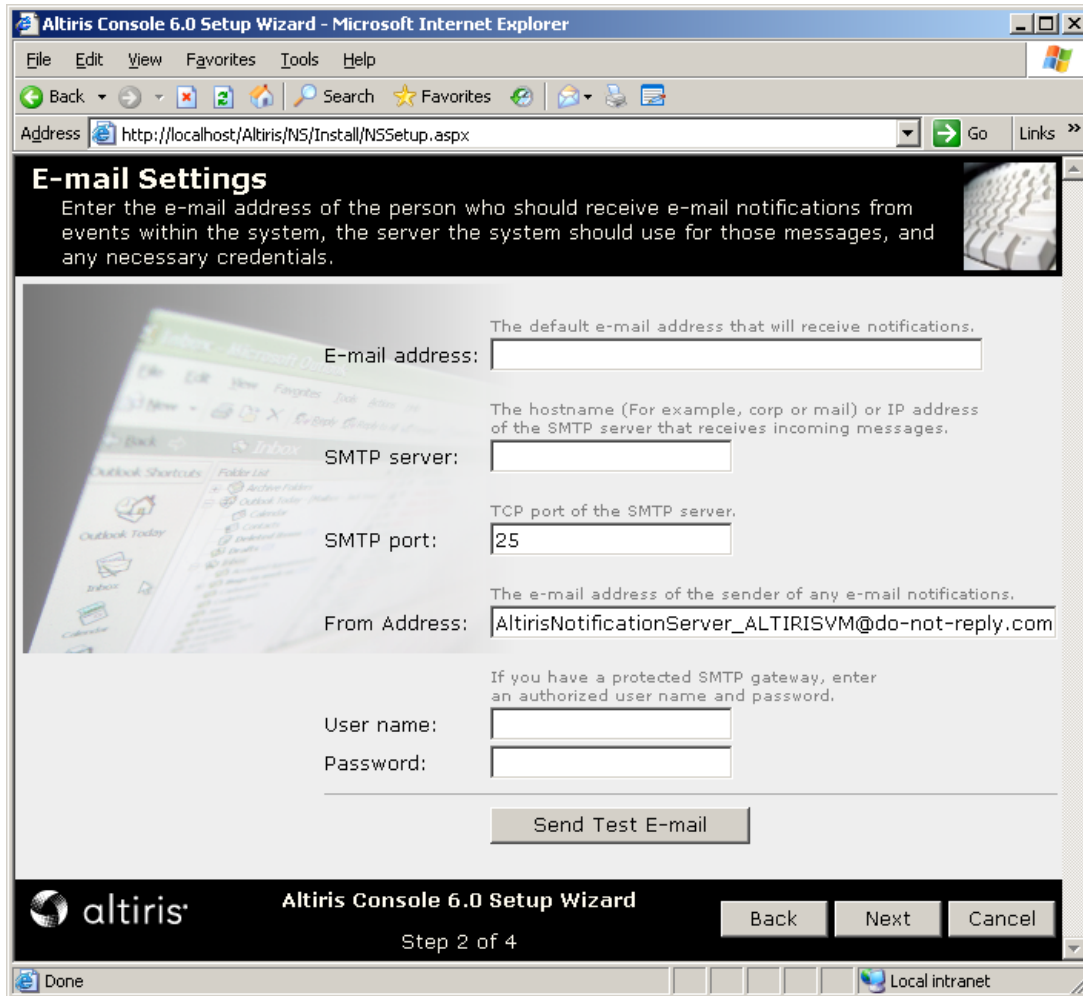


Figure 8-6 The E-mail Settings page of the Notification Server configuration process

3. The SQL Database Settings page lets you set up credentials for Microsoft SQL Server and the installed Notification Database. Enter the name of the server running Microsoft SQL Server or MSDE. You can install the Notification Database to a specific SQL 2000 instance by entering the server name and SQL instance (Example: SQL server name\SQL instance.). Select **Create new database** and give the database a name.

Enter a value between 1 and 3600 seconds (1 hour) in the text box labeled **Command timeout**. The command timeout setting applies to all SQL Server connections used by the Notification Server. If you experience timeout errors

when using a database connection, due to network traffic or heavy server usage, increase the value of this setting. Click **Next** to continue.

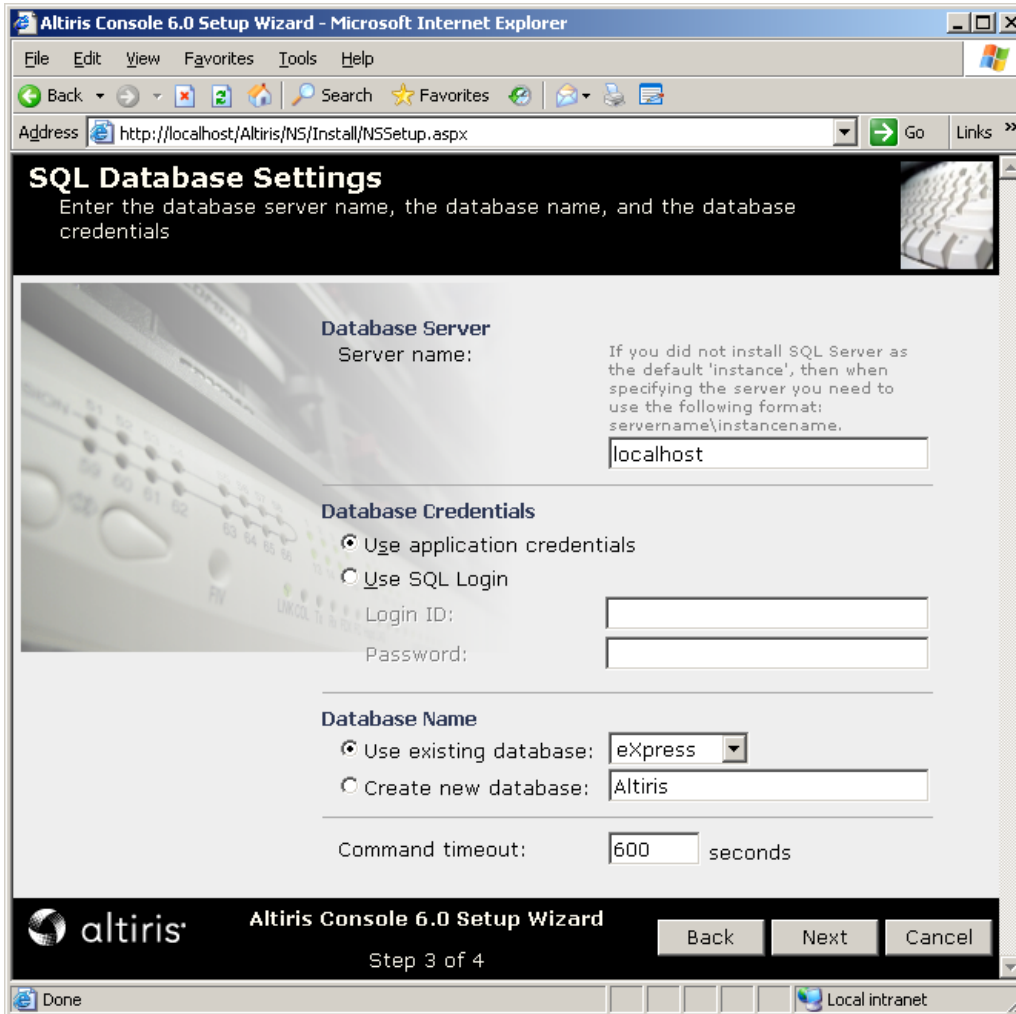


Figure 8-7 The SQL Database Settings page of the Notification Server configuration process

4. On the final summary page, click **Finish** to complete Notification Server configuration. A notification window will appear informing you that the Notification Server will be paused while configuration takes place.

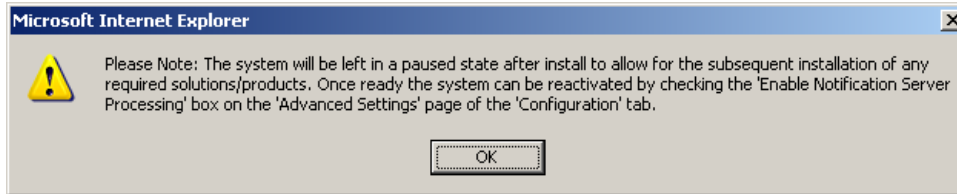


Figure 8-8 A notification window at the end of the Notification Server configuration process

5. After the installation and configuration is complete, the Altiris Console can be launched from the Altiris folder in the Windows Start menu. Shown in Figure 8-9.

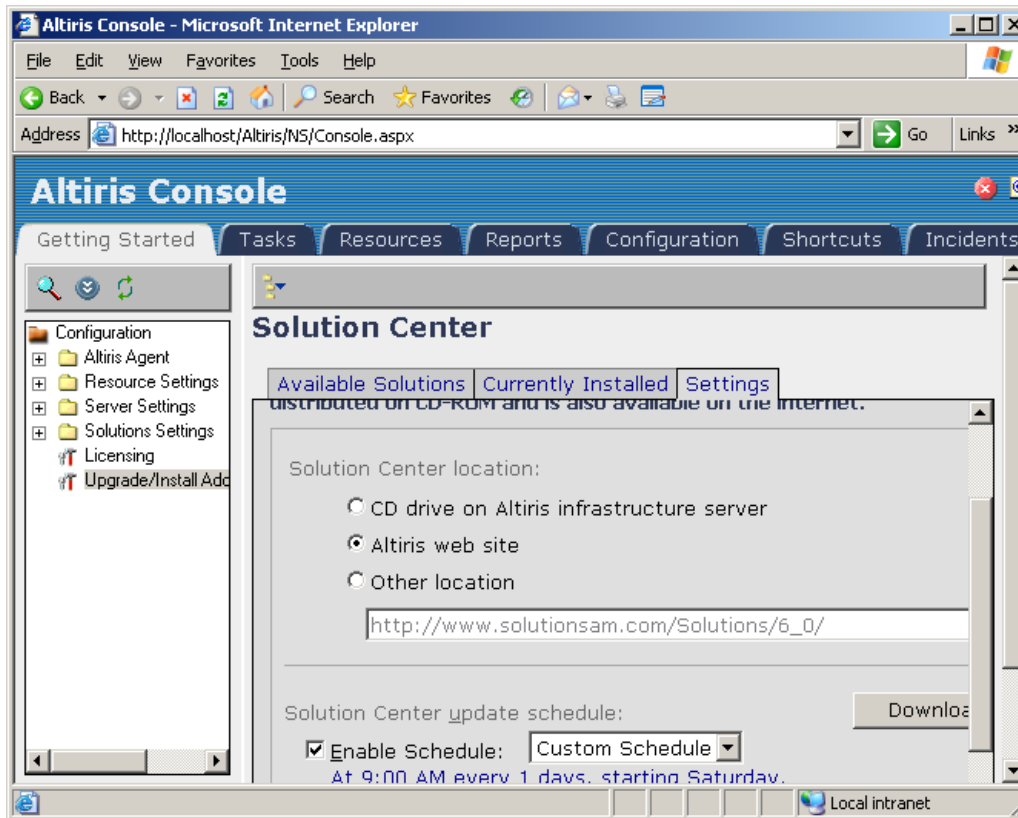


Figure 8-9 The Altiris Console

8.2.2 Altiris Connector Solution 6.1

Altiris Connector Solution is a tool used to transfer data between numerous external data sources and the Notification Database. This allows you leverage data that already exists in other applications. The scheduling capabilities of Connector Solution allows you to regularly and automatically re-transfer data, so data in the Notification Database and external data sources can easily be kept current.

Connector Solution supports many data formats. Many of these formats are supported by built-in functionality, such as OLE, ODBC, LDAP, XML, and CSV. Other formats are supported through the addition of Connector Packs. A Connector Pack is an add-on to Connector Solution that lets you transfer data and events between Notification Server and an application not supported with built-in Connector Solution functionality. Connector Packs are available for applications such as IBM Director, HP OpenView, Remedy, and Wise Package Studio.

Note: This document assumes a working knowledge of Altiris Connector Solution. For more information about Connector Solution refer to the *Altiris Connector Solution 6.1 Product Guide* available at the following URL:

<http://www.altiris.com/upload/connector.pdf>

For a list of Connector Packs currently available, visit the Altiris Web site at the following URL:

<http://www.altiris.com>

Installing Connector Solution 6.1

Connector Solution is installed from the Altiris Console.

To install Connector Solution follow the steps outlined below:

1. From the Altiris Console, click the **Getting Started** tab.
2. Click the link labeled **Install Altiris Solutions from the Solution Center**, which is located in the upper-left portion of the page.

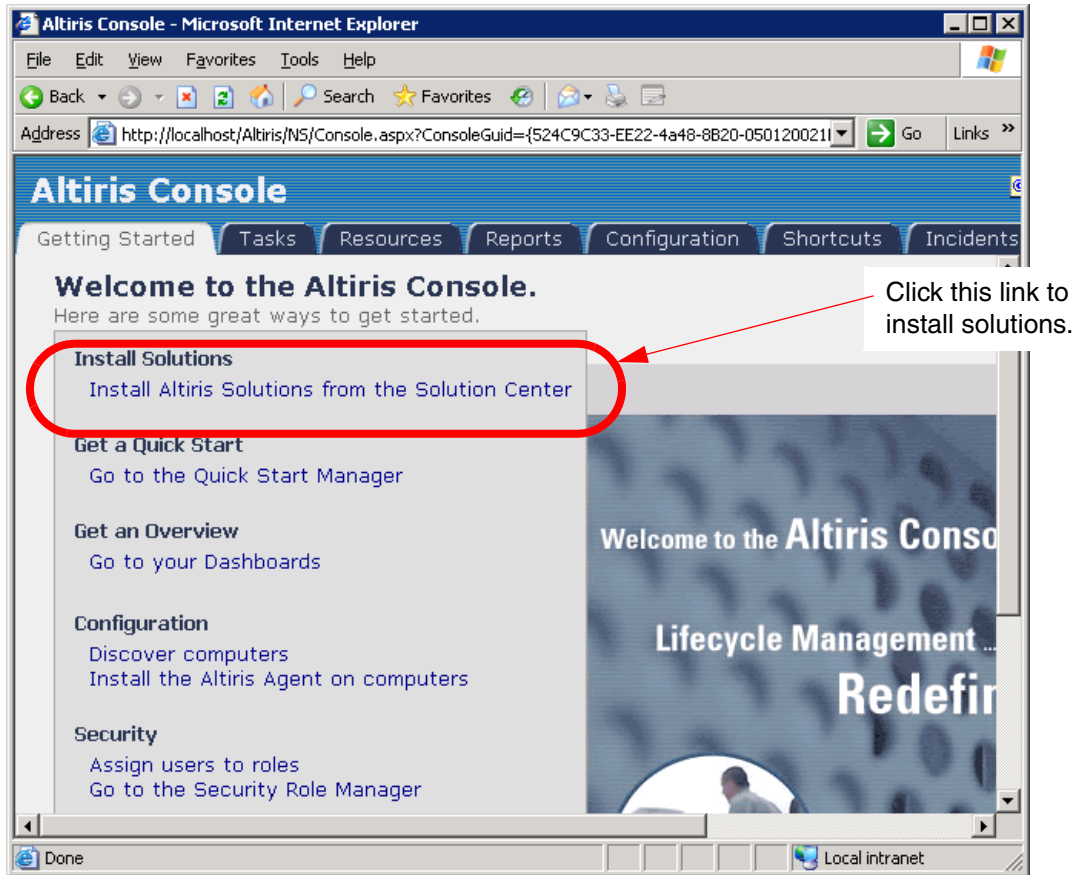


Figure 8-10 The Getting Started tab of the Altiris Console

3. Clicking the link opens the Configuration tab and the **Upgrading/Install Additional Solutions** option. If the solutions download portal has not been configured, you will be presented with the configuration page.

There are three source options for downloading Altiris solutions: using a CD on the Altiris infrastructure server (the computer running Notification Server), the Altiris Web site, or another location. The easiest method is to use the Altiris Web site by selecting **Altiris Web site**. However, if your Notification Server does not have an active Internet connection, you can use the CD drive on the Notification Server by selecting **CD drive on Altiris infrastructure server** or you can use a file share by selecting **Other location**. In our test environment the Notification Server did not have an Internet connection. To configure the solutions download source we used a Web site ripping tool to download the entire contents of the Altiris solutions Web site and burned the contents to a DVD.

When you have made your selection, scroll down the page and click **Apply**.

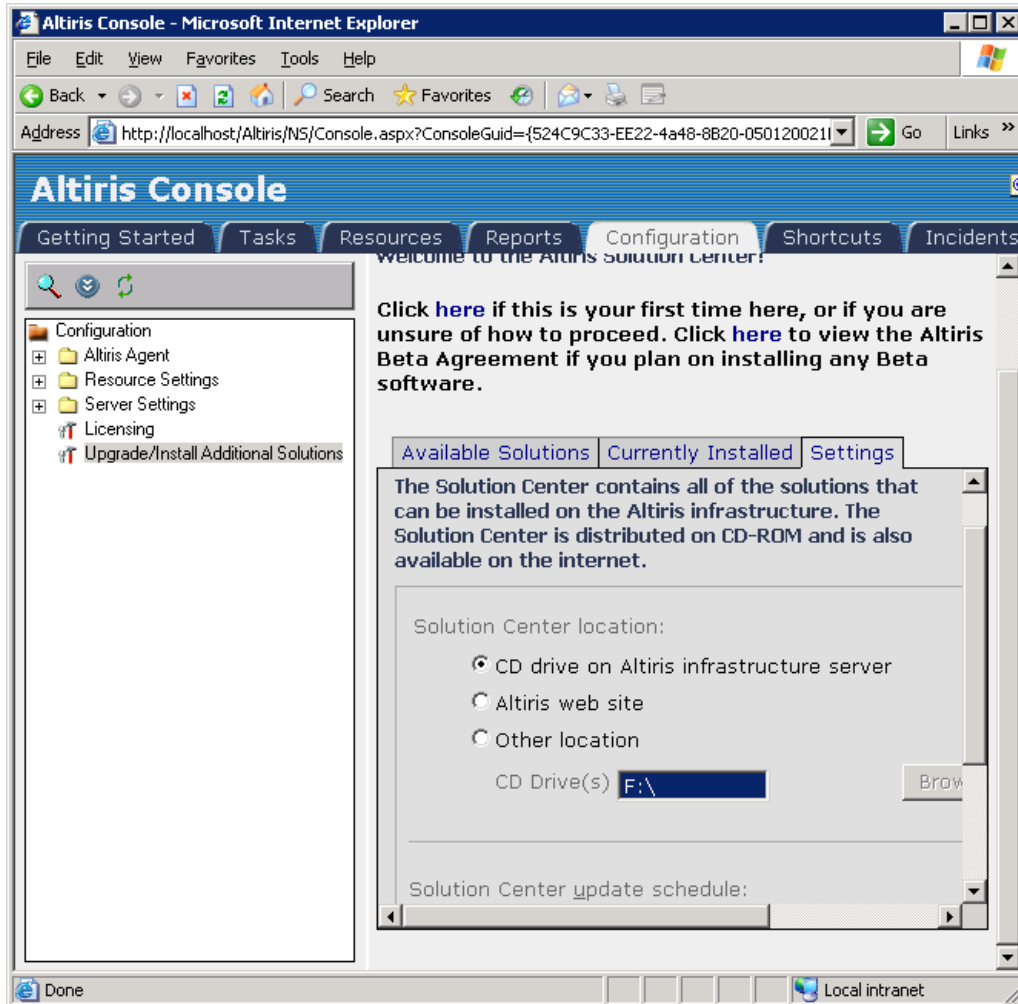


Figure 8-11 Configuring the source for Altiris solutions download

4. Once you have configured the source for the download, click the **Available Solutions** tab in the details pane of the Altiris Console.
5. On the Available Solutions tab, click the **Solutions**. This lists the solutions that can be downloaded and installed on your Notification Server.

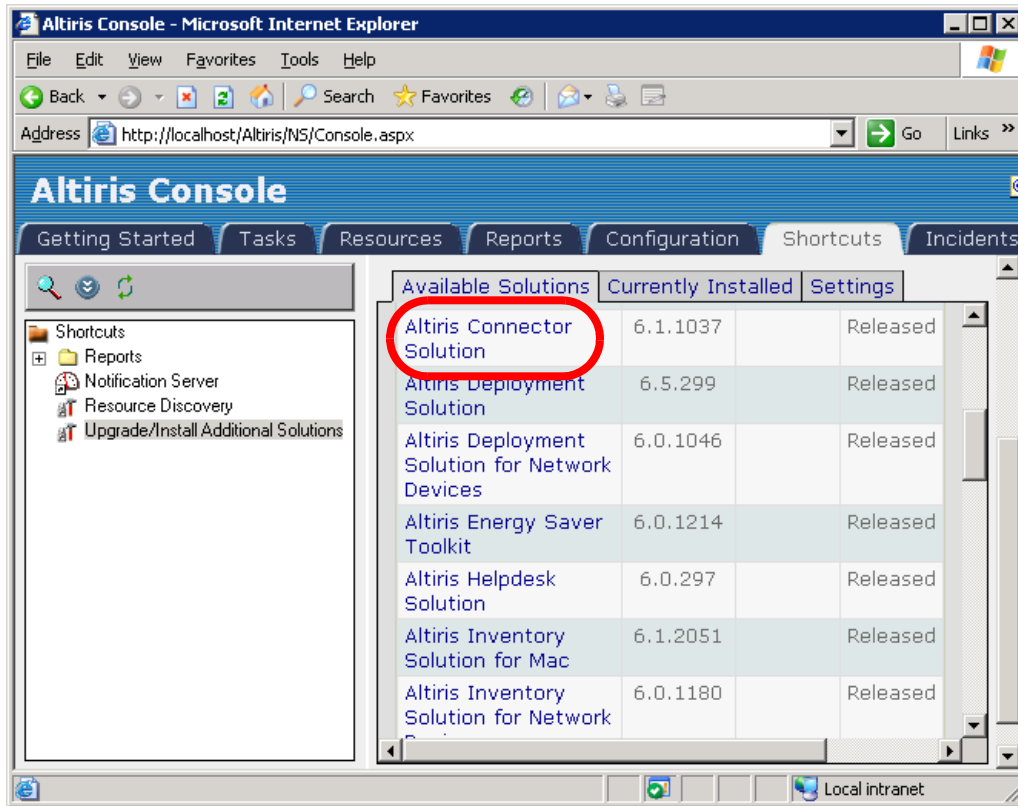


Figure 8-12 The Altiris Console listing the various solutions available for download

6. To install Connector Solution scroll down the list of solutions until you find the solution named **Altiris Connector Solution**. Click the link to initiate the installer. A summary window will appear listing the various components that will be installed.

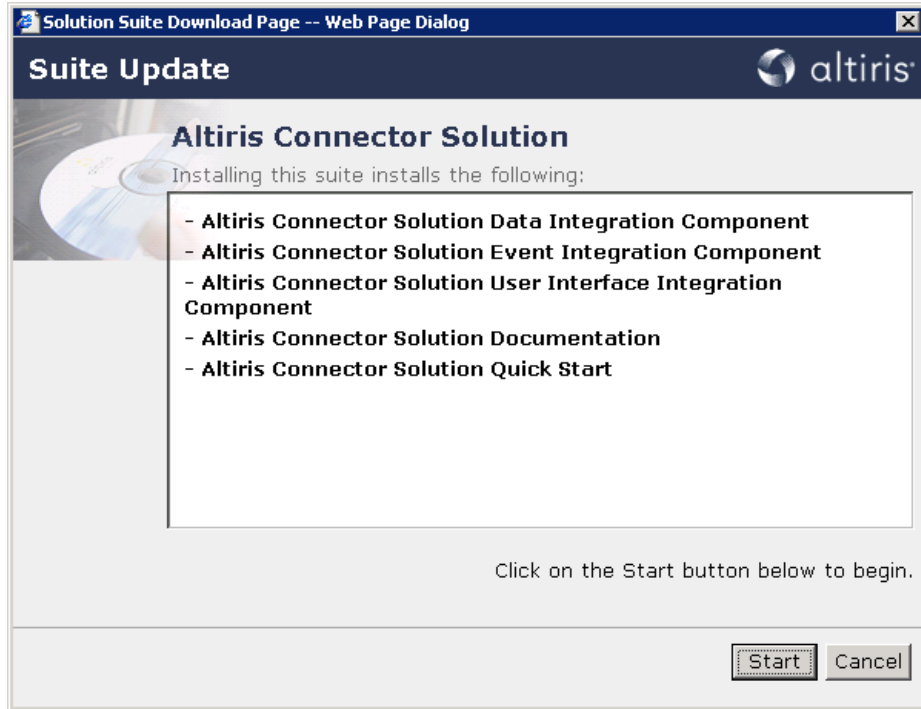


Figure 8-13 A summary window listing the various components that will be installed

7. Click **Start** to begin installing Connector Solution.
8. When the installation completes, click the **Currently Installed** tab in the details pane of the Altiris Console to verify that Connector Solution has been installed.

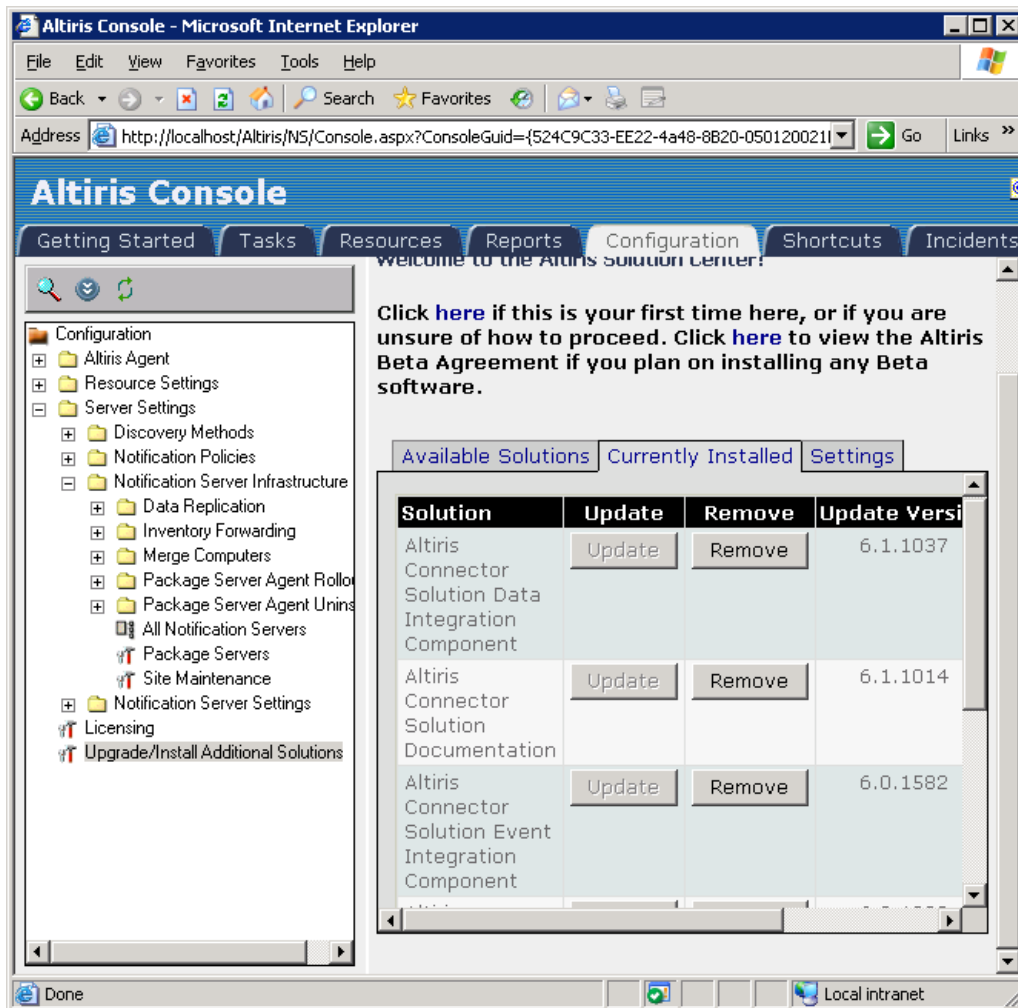


Figure 8-14 The Currently Installed tab showing the installed Connector Solution components

8.2.3 Altiris Connector for IBM Director

The Altiris Connector for IBM Director is an add-on to Connector Solution that allows organizations to extend their investment in the IBM Director platform. The Connector for IBM Director allows Connector Solution to share data between IBM Director and Notification Server. With the Connector for IBM Director, users can access Notification Server inventory data directly through the IBM Director console and can access IBM Director collected data from the Altiris Console.

The Connector for IBM Director is a no-charge download that is available on the Altiris Web site.

Note: The Connector for IBM Director supports IBM Director version 5.10 or higher.

Connector for IBM Director integrates with IBM Director by providing the following functionality:

▶ Data integration

With data integration you can create a link between the Notification Database and IBM Director's database. Using an import feature in Notification Server you can then import information saved in IBM Director's database into the Notification Database. By providing connection details and security credentials you can set a schedule for recurring data import.

Once data from IBM Director has been integrated with Notification Server, Notification Server can then generate reports that include more IBM specific information.

▶ Event integration

The event integration between IBM Director and the Altiris infrastructure is built on Connector Solution components. The event integration module of Connector for IBM Director lets you send management information between IBM Director and Notification Server. The event integration module uses SNMP to communicate the events.

The SNMP event integration module provides the following functions:

- Receiving of SNMP traps from the network and places them in the Notification Database.
- Sending of SNMP traps (using SNMP automated actions) using data from the Notification Database to SNMP listeners in the network.
- Enabling or disabling SNMP trap events targeted at IBM Director managed computers.

Note: The Connector for IBM Director includes Management Information Base (MIB) database files for interpreting received SNMP trap events that are required by IBM Director. The task of importing the MIBs into IBM Director requires some manual steps.

MIB is a database of objects that can be monitored by a network management system. Both SNMP and RMON use standardized format that allows any SNMP and RMON tools to monitor any device defined by a MIB.

For more information about MIBs and importing MIBs into IBM Director, reference the Director documentation, which is available on the IBM Director 5.1 installation CD or the IBM Redbook, *Implementing IBM Director 5.10*, SG24-6188.

► User interface integration

A number of tasks are added to the IBM Director console that allow many functions of the Altiris Console to be launched directly from the Director console. The UI integration between IBM Director and the Altiris Infrastructure is built on Connector Solution components.

Installing the Connector for IBM Director

The Connector for IBM Director is installed the same way as Connector solution. Review the install process outlined above in “Installing Connector Solution 6.1” on page 262.

To install the Connector for IBM Director follow the steps outlined below:

1. From the Altiris Console, click the **Getting Started** tab.
2. Click the link labeled **Install Altiris Solutions from the Solution Center** which is located in the upper-left portion of the page.
3. Since the source for the solutions download was configured when we installed Connector Solution, we do not need to configure the settings again. Click the **Available Solutions** tab in the details pane of the Altiris Console. On the Available Solutions tab, click **Segments**. This lists various categories for the various downloads.

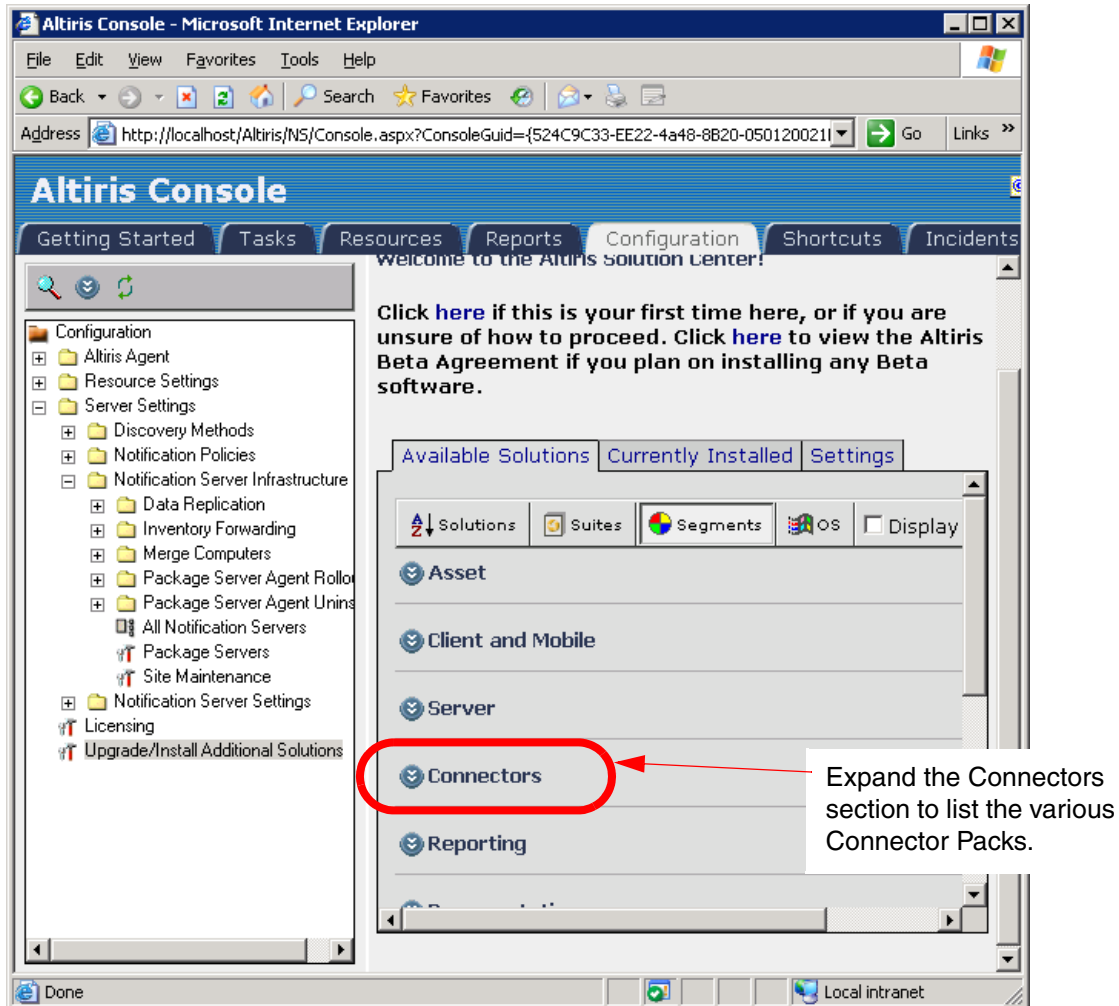


Figure 8-15 The Segments section showing the various categories of solution downloads

4. Expand the category labeled **Connectors** and scroll down until you see the link labeled **Altiris Connector Pack for IBM Director**. Click the link to initiate the install.

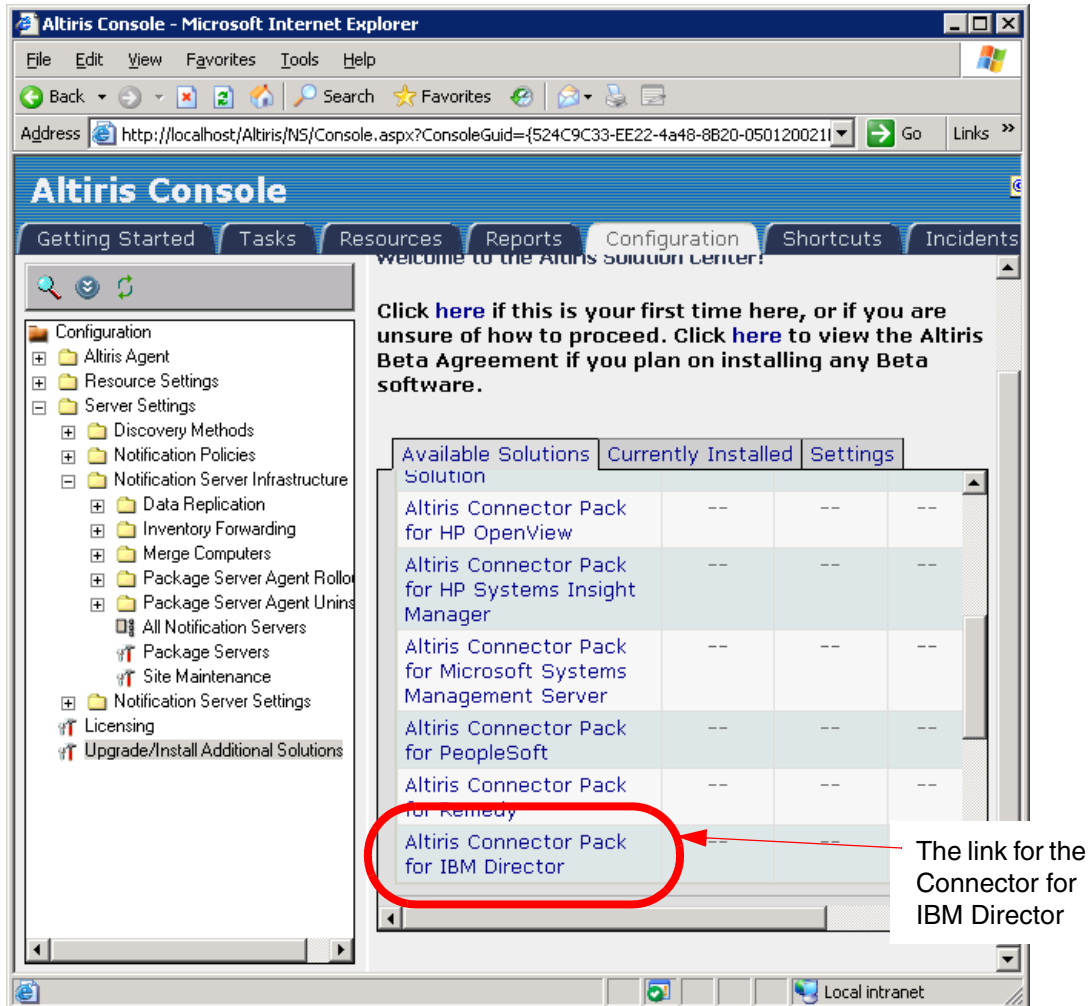


Figure 8-16 The Altiris Console listing Connector Packs that can be downloaded and installed

5. A summary window appears showing the various components that will be installed. Click **Start** to begin the installation.

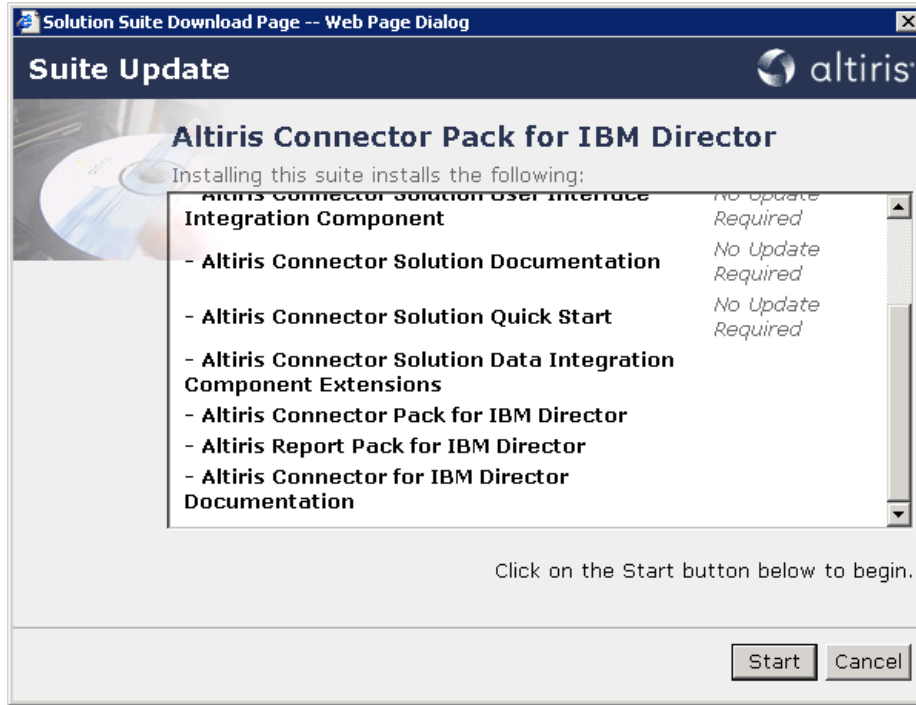


Figure 8-17 A summary window showing the various components that will be installed

- Once the download completes, click the **Currently Installed** tab to verify the Connector for IBM Director installed.

8.2.4 Connector Agent for IBM Director

The Connector Agent for IBM Director is the communication link between the Notification Server and IBM Director. The agent installs files and folders on your IBM Director server that are required for performing event and user interface integration with IBM Director. It must be installed on the IBM Director server computer and must be installed before the Connector for IBM Director will work. However, it cannot be installed until after you install the Connector for IBM Director.

Before installing the Connector Agent for IBM Director, computers must be added to the computers collection in the Notification Database.

Adding Computers to IBM Director

Before using the full feature set of the Connector for IBM Director, you must add the computers saved in the Director database to the IBM Director Computer's Collection in the Altiris Console.

Tip: Notification Server refers to computers as *resources*.

Add computers to the Notification Database by following the steps outlined below:

1. From the Altiris Console, select the **Configuration** tab.
2. In the tree-view pane select **Solutions Settings** → **Connectors** → **IBM Director** → **IBM Director computers**. Click the **Edit Collection** icon.

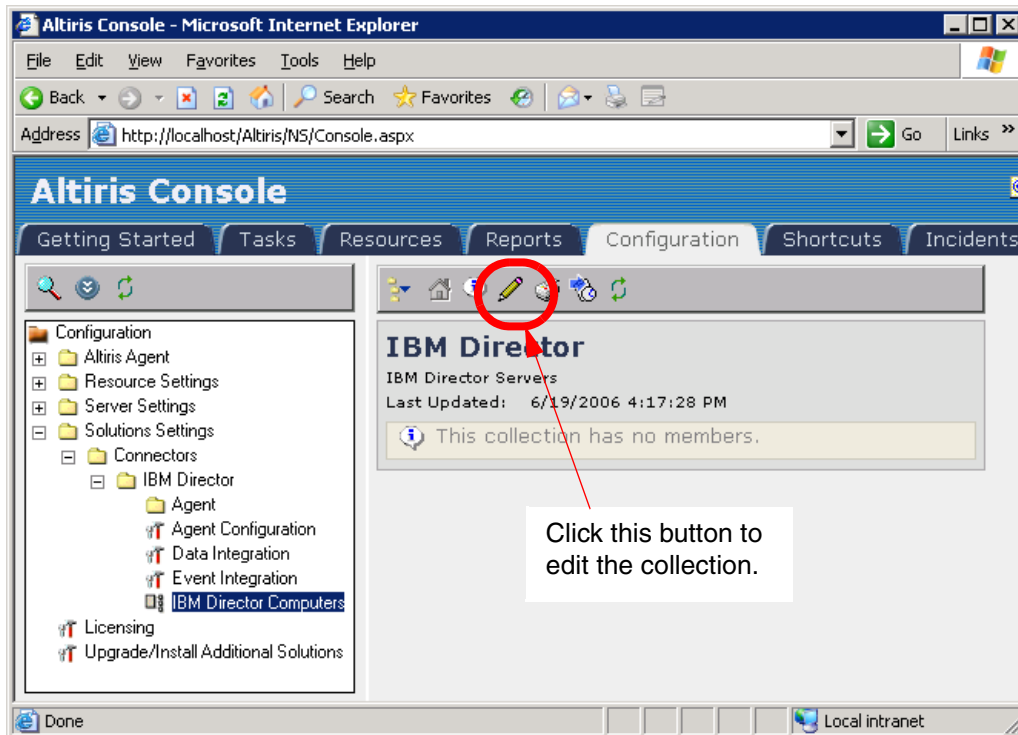


Figure 8-18 Initially the IBM Director Computers collection does not have any members

3. In the Inclusions section of the page, click the link labeled **Select a resource**.

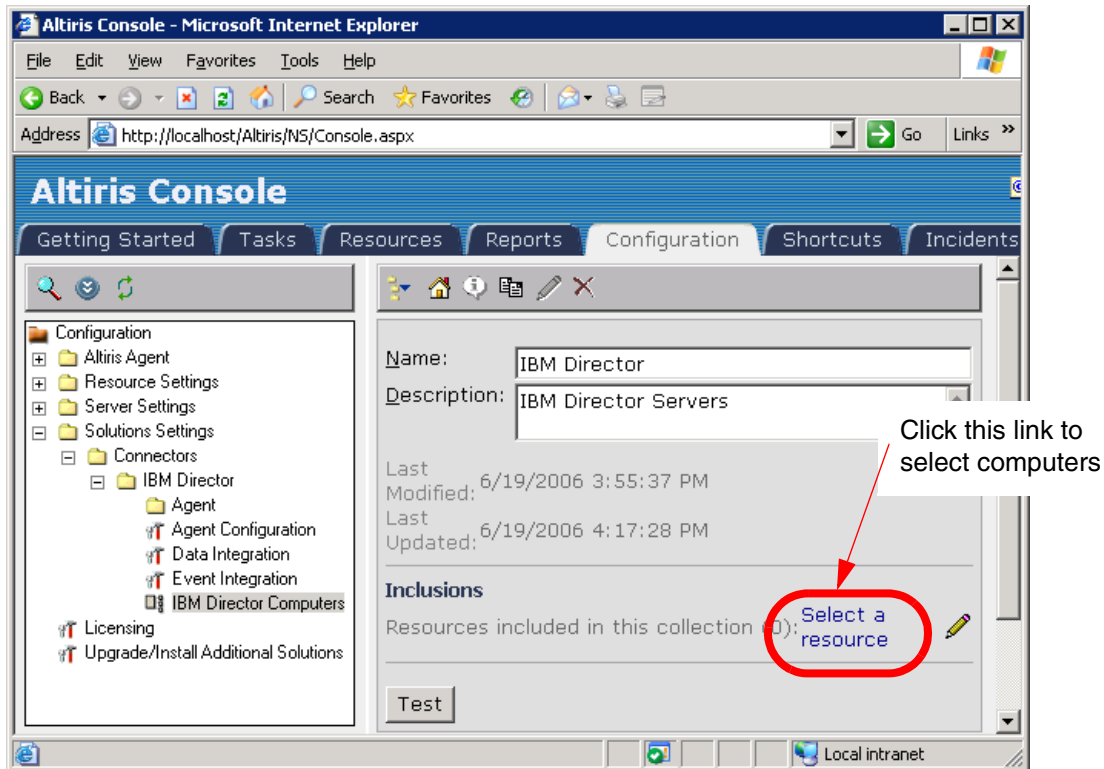


Figure 8-19 Click the Select a resource link to select computers

4. On the Find a Resource window, you have four pull-down menus for selecting different criteria to use when searching for computers to add as resources. If you want to search by domain, operating system name, server type, or NetBIOS name, use the pull-down lists to fine-tune your search.

Once you have narrowed down your search criteria, click **Find** to search for computers. When computers are found, they appear in a list box toward the middle of the Find Resource window. Select the computers you want to add and click **OK** at the bottom of the window.

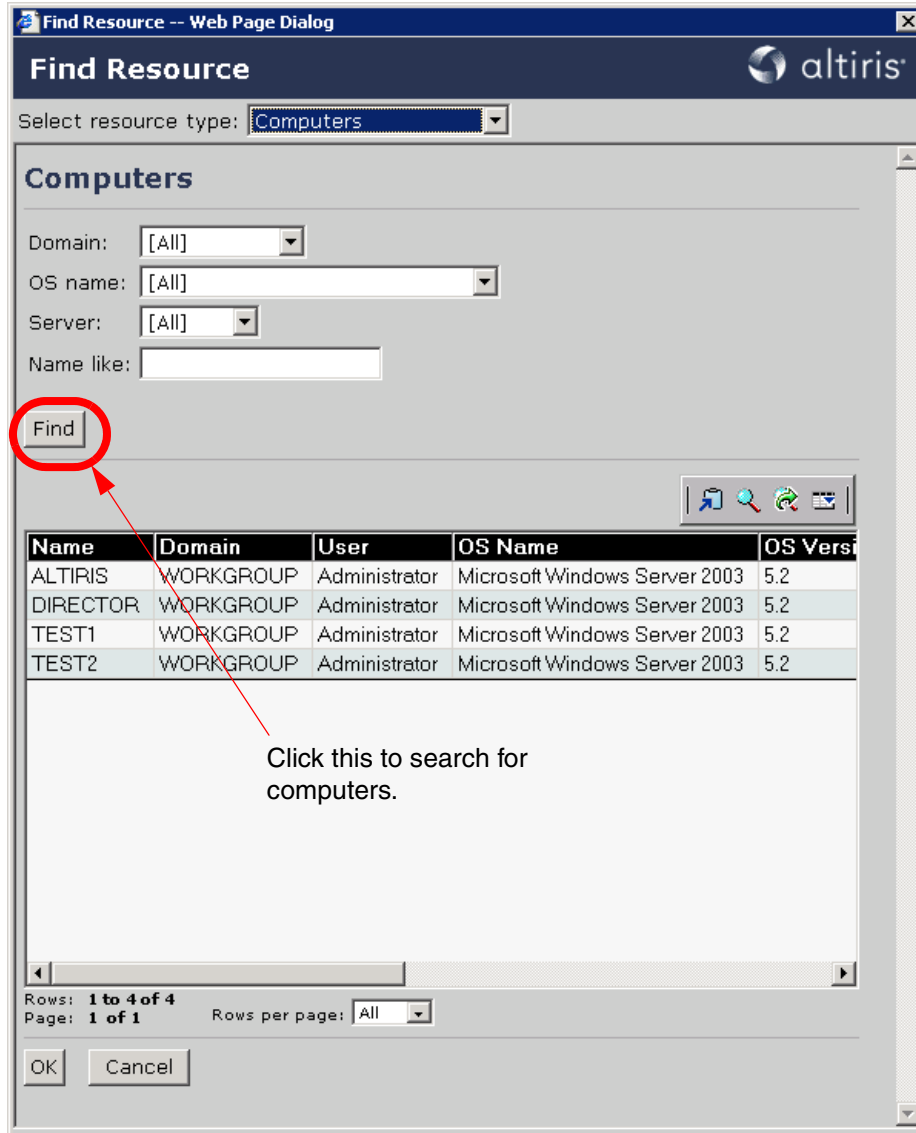


Figure 8-20 The Find Resource window after finding numerous computers

5. On the Selector window, select the computers you want to add as resources and click **Add a resource**.

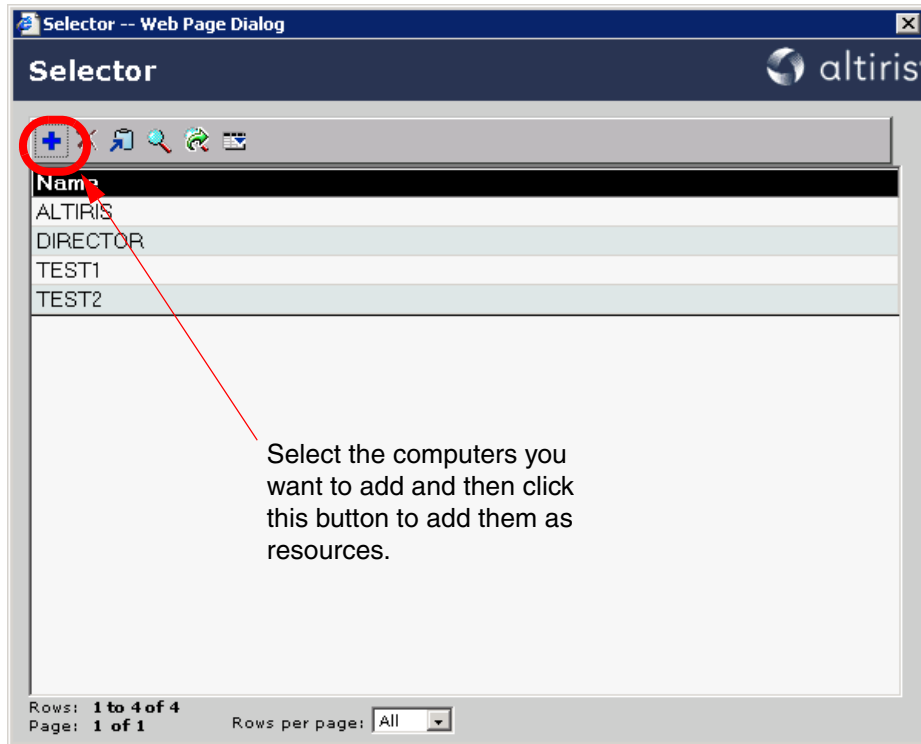


Figure 8-21 The Selector window showing the discovered computers

6. Click **OK** to close the Selector window, click **OK** to close the Find Resource window, then click **Apply**.

Now that computers have been added to the Notification Database as resources, the Connector Agent for IBM Director can be installed.

Installing the Connector Agent for IBM Director

To install the Connector Agent follow these steps:

1. From the Altiris Console, click the **Configuration** tab.
2. In the tree pane, select **Solutions Settings** → **Connectors** → **IBM Director**.

3. In the details pane of the Altiris Console, double-click **Agent Configuration**.

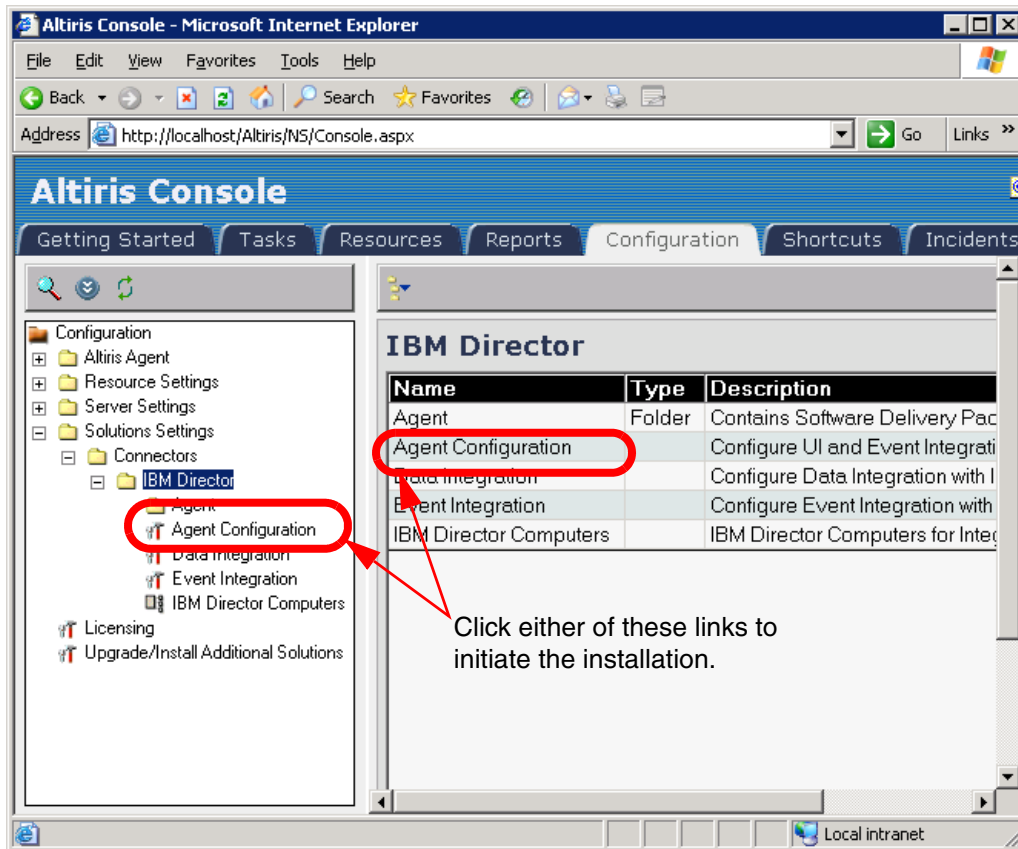


Figure 8-22 The IBM Director page showing multiple functions

4. Install the agent automatically by using the pull-down menu for **Select an IBM Director Computer** to select the computer on which to install the Connector Agent. When you have selected the computer, click **Configure Software Delivery** to create a Director task.

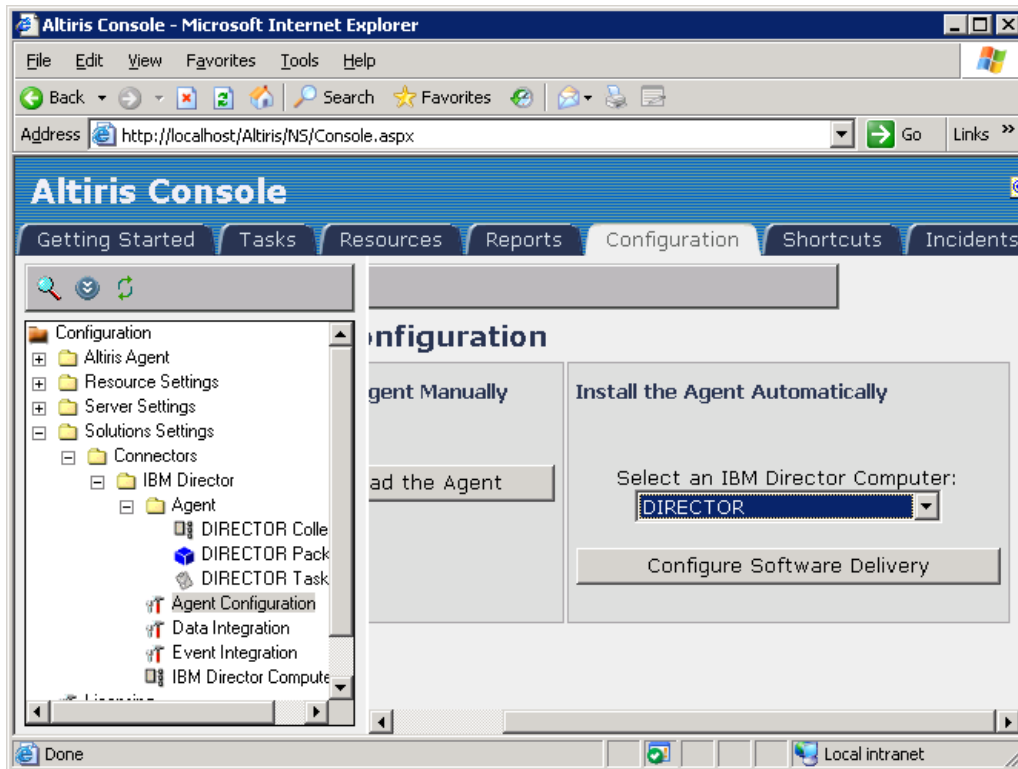


Figure 8-23 The Agent Configuration window

- The Task window shows various settings that can be configured regarding Connector Agent deployment. Settings include disabling multicast and scheduling the task run time. If you want to run the agent install right away, select **Run once ASAP**. Complete the setup by clicking **Apply** at the bottom of the Task window. If you selected to run the task now, the agent install will begin shortly. If you choose to schedule the task to run at a later time, the task schedule will be saved and the install will execute at the specified time.

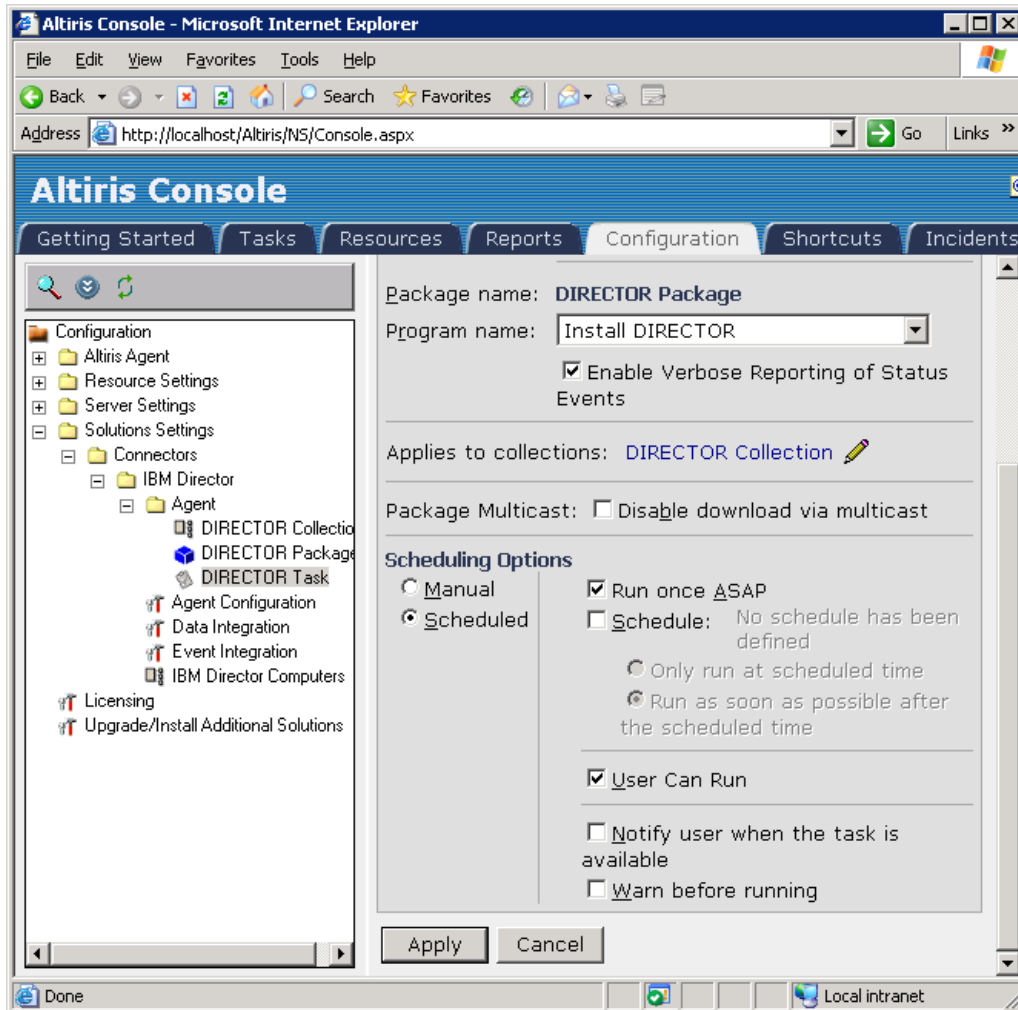


Figure 8-24 The Task window showing task information

Note: To verify that the Connector Agent has installed on the IBM Director server computer, go to Add/Remove Programs of the computer and verify that there is a program called Altiris Connector for IBM Director Agent.

8.2.5 Final configuration

Once the major components have been installed, some final configuration needs to take place to complete the upward integration.

User interface integration

After you have finished installing the Connector Agent for IBM Director, you can view the user interface changes made to the Director console. The additional tasks can be located in the Tasks pane of IBM Director Console, under the Altiris heading.

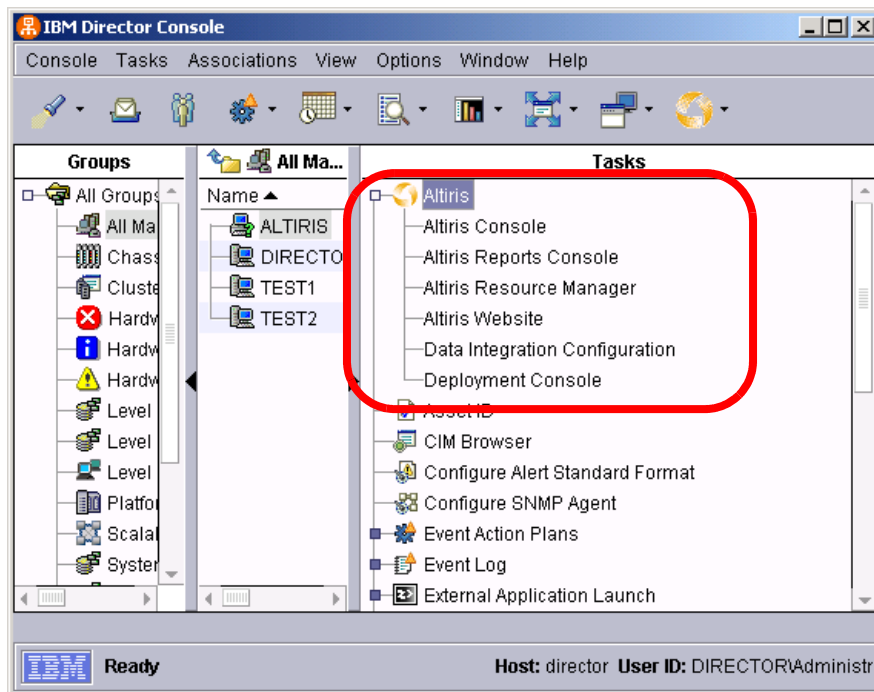


Figure 8-25 IBM Director Console showing the added tasks

The following table gives a brief explanation for the tasks that are added to Director Console.

Table 8-1 Additional tasks added to Director Console

Component	Description
Altiris Console	Opens the Altiris Console
Altiris Reports Console	Opens the Altiris Console to the Reports tab
Altiris Resource Manager	Opens Resource Manager in the context of a single computer. This only opens if a computer resource is selected or dragged to the Altiris Resource Manager link.
Altiris Web Site	Opens the Altiris Web site
Data Integration Configuration	Opens the Altiris Console with the Basic Data Import page displayed.
Deployment Console	Opens the Altiris Console to the Deployment tab

Note: To launch the Altiris Resource Manager tool, a computer must first be selected in the computers pane of the Director console. An alternate method for launching this tool is to right-click the computer and select **Altiris** → **Altiris Resource Manager** from the context sensitive menu.

Compiling Altiris MIBs

When the Connector Agent for IBM Director was installed on the Director server, a number of MIB files were also saved on the Director server.

Before configuring event integration, the MIB files must be integrated into the Director server.

Note: Management Information Base (MIB) is a database of objects that can be monitored by a network management system. Both SNMP and RMON use standardized format that allows any SNMP and RMON tools to monitor any device defined by a MIB

To integrate the Altiris MIBs into IBM Director follow the steps outlined below:

1. From IBM Director Console, on the main menu select **Tasks** → **SNMP Browser** → **Manage MIBs**. This will open the MIB Management window.

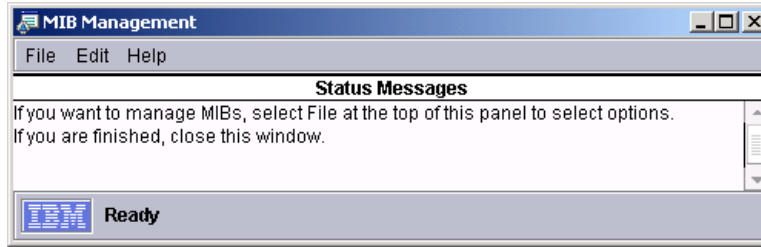


Figure 8-26 The MIB Management window

2. From the main menu of the MIB Management window, select **File** → **Select MIB to compile**.
3. From the list box on the left pane of the window, select **altiris-custom-mib_6_0.mib** and click **OK**.

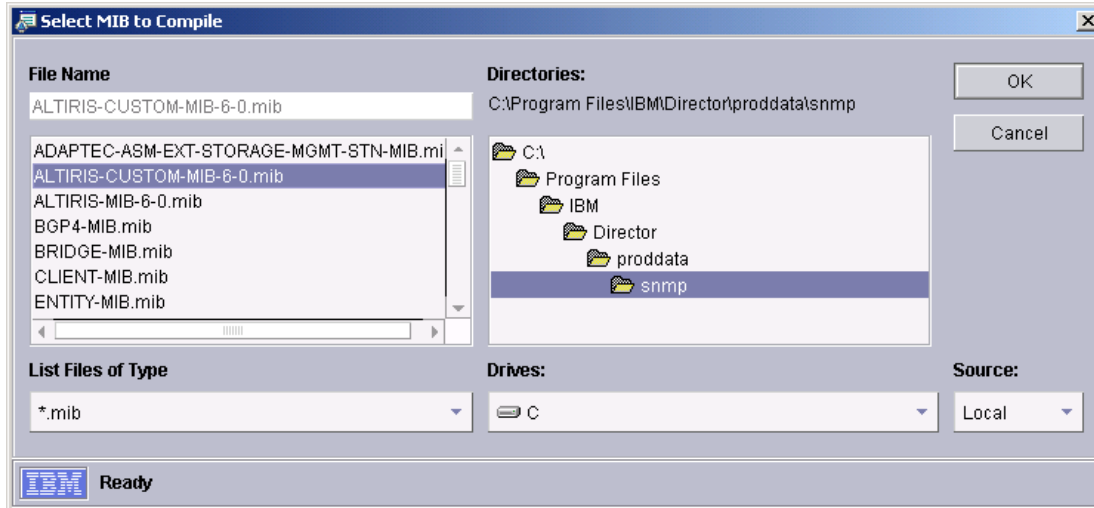


Figure 8-27 The Select MIB to Compile window

4. Once the MIB compiles, repeat Steps 2 and 3 for any remaining Altiris MIB files.
5. Close the MIB Management window when you are finished.

Now that you have compiled the MIBs, you can configure event integration.

Event integration

The event integration module of Connector Solution with the Connector for IBM Director lets you send management information between IBM Director and the

Notification Server. The event integration module uses SNMP to communicate the events.

The SNMP event integration module provides the following functions:

- ▶ Receiving of SNMP traps from the network and places them in the Notification Database.
- ▶ Sending of SNMP traps (using SNMP automated actions) using data from the Notification Database to SNMP listeners in the network.

SNMP listeners are required for event integration. SNMP listeners must be added before setting up Event Integration in Notification Server.

The event integration with Notification Server and IBM Director is a complex process and is beyond the scope of this redbook. For more information about adding event listeners and configuring event integration, reference the following documents:

Connector Solution 6.1 Product Guide which can be found at the following URL:

<http://www.altiris.com/Support/Documentation.aspx>

Connector Pack 6.0 for IBM Director Product Guide which can be found at the following URL:

<http://www.altiris.com/upload/connectoribmdirector.pdf>

Data integration

The most common form of data integration is to link the Notification Database with the IBM Director database so they can share inventory and related information. When the link is established, you can access data from both databases from the IBM Director console or from Altiris Notification Server.

At this time, SQL Server 2000 with Service Pack 3 is supported. However, you should be able to establish a link to most databases from this page.

To establish a SQL Server database link:

1. From the Altiris Console, select the **Configurations** tab.
2. In the tree-view pane select **Solution Settings** → **Connectors** → **IBM Director** → **Data Integration**. This will load the Basic Data Imports page.

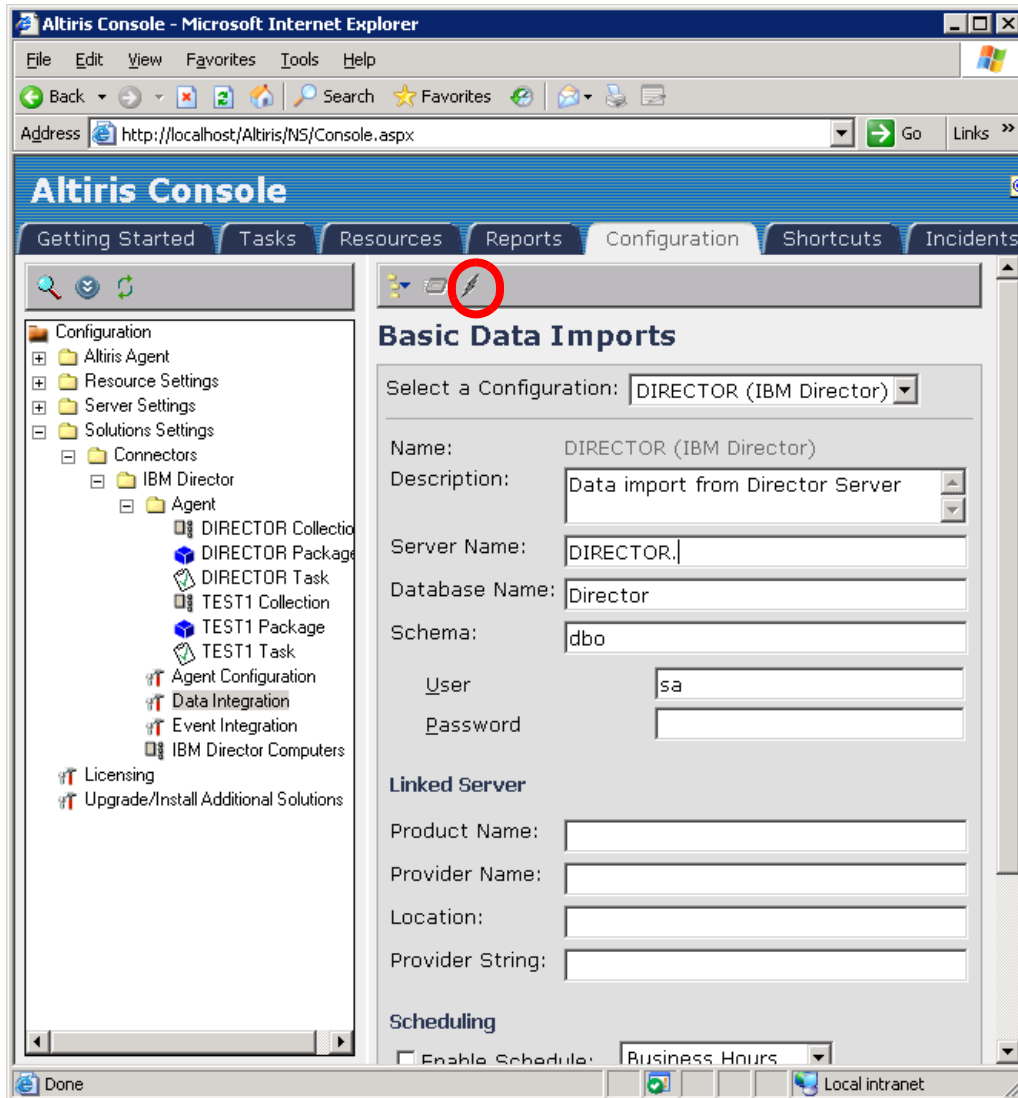


Figure 8-28 The Basic Data Imports window with the Test configuration button highlighted

3. From the pull-down list for **Select a Configuration**, choose the computer that is your IBM Director database server. In the **Description** text box, type a description for your configuration.
4. In the **Server Name** field, type the NetBIOS name of the Director database server. In the **Database Name** field, type the name of the database that holds the IBM Director information. If you want to use a specific schema, enter it in the **Schema** text box.

5. Enter a user account name with rights to access the Director database in the **User** text box followed by that user's password in the **Password** text box.
6. In the **Product Name** text box, enter:
SQLServer OLEDB provider
7. In the **Provider Name** text box, enter:
SQLOLEDB
8. The next two text boxes do not require any text when using SQL Server.
9. Finally, if you want to create a reoccurring schedule for data import, select **Enable Schedule** and use the pull-down list to determine the time to perform the import.
10. Click **Apply** to establish the link.
11. Click the **Test configuration** icon (see Figure 8-28 on page 284) on the toolbar to test the configuration and then scroll to the bottom of the page to view any informational messages. If the test is unsuccessful, an error message will be displayed.

In addition to linking the two databases, you can also import computer resources from the IBM Director database to the Notification Database. The computer name and a computer identifier are all that get uploaded to the Notification Server. For every computer stored in the IBM Director database, a resource is created (if it does not already exist) in the Notification Database. Once the resources have been imported, reports and various tasks can be targeted towards these computers.

There are two methods of importing computer resources:

- ▶ Click the **Run the Selected Configuration** icon (see Figure 8-29 on page 286) on the tool bar to import immediately; or
- ▶ Select **Enable Schedule** toward the bottom of the Basic Data Imports page and define the schedule to run the import by using the pull-down list. After you click **Apply**, the import will run at the defined time.

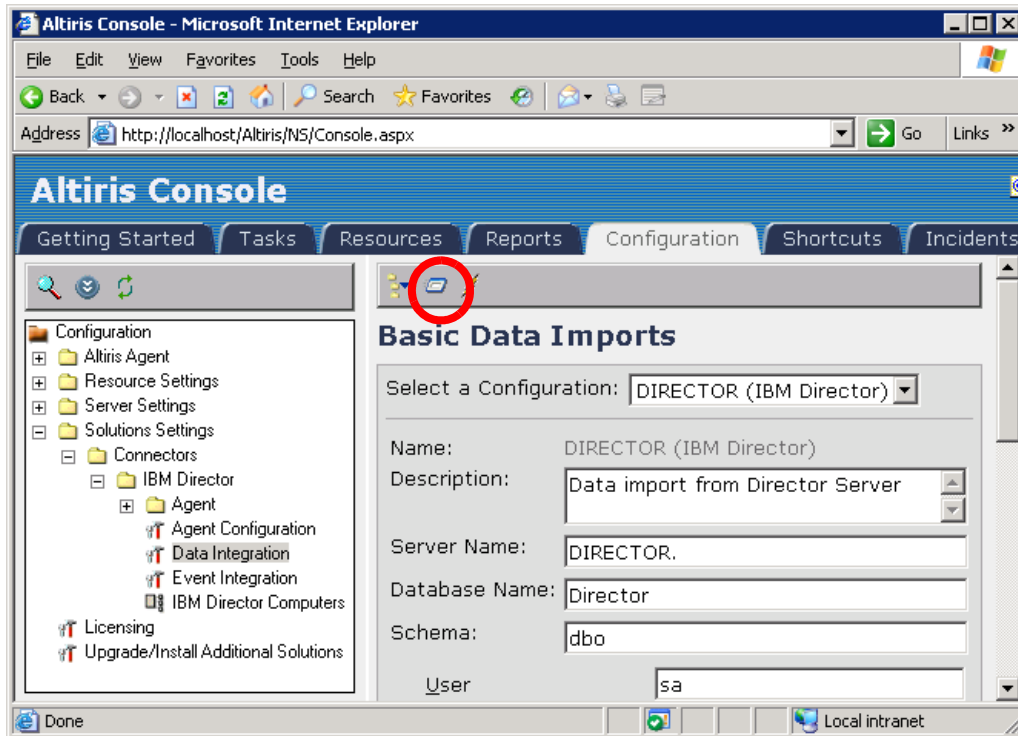


Figure 8-29 The Basic Data Imports page with the Run the Selected Configuration icon highlighted

Running reports from the Altiris Console

After creating a link between the Notification Database and IBM Director's database and importing computer resources, you can run several reports to view data collected by IBM Director directly from the Altiris Console.

To run a report follow the steps outlined below:

1. From the Altiris Console, click the **Reports** tab.
2. In the tree-view pane, select **Reports** → **Connector** → **IBM Director**. Next click one of the reports in the IBM Director folder.

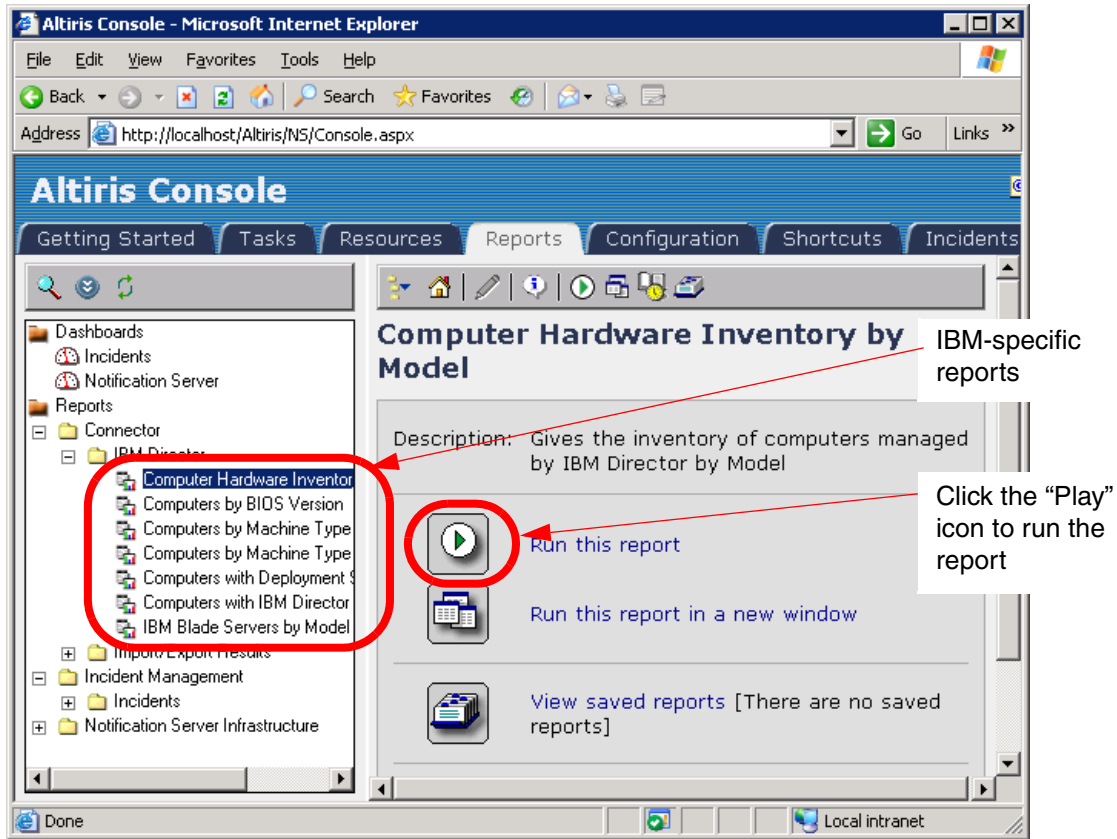


Figure 8-30 The Reports tab of the Altiris Console

3. To run the selected report, click the **Play** icon in the details pane.

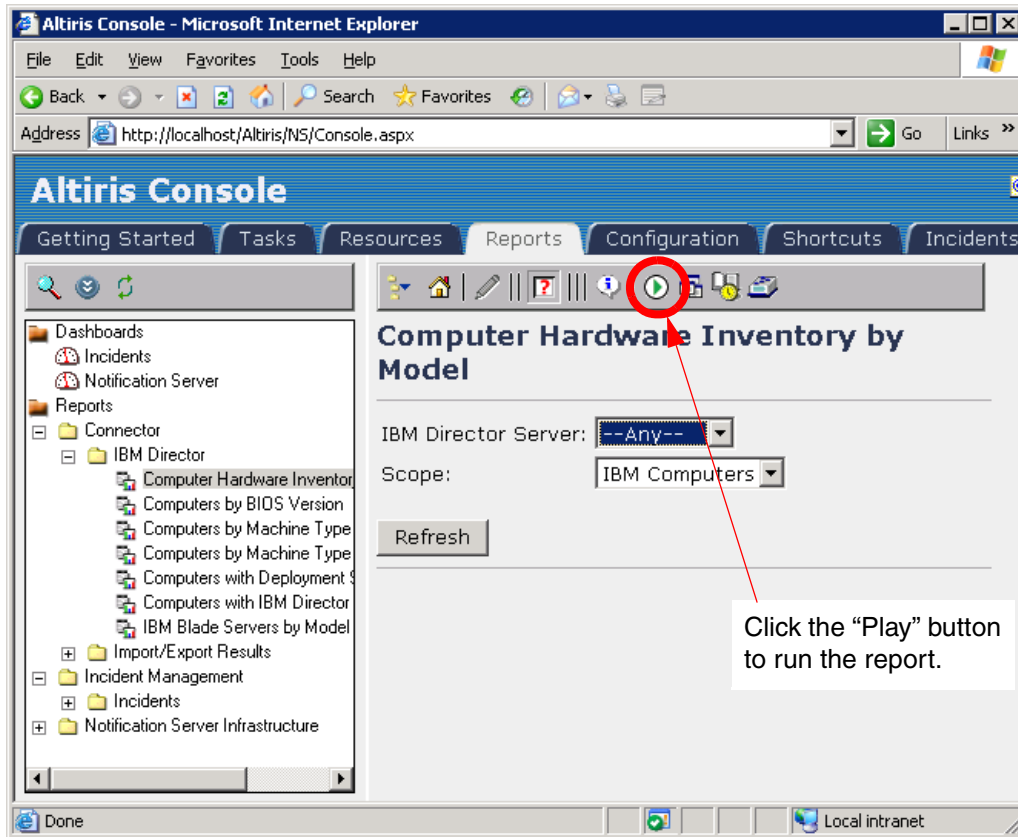


Figure 8-31 The Reports tab of the Altiris Console showing pull-down lists to limit report

4. In the details pane, there will be a number of pull-down lists. Use these to define the scope of the report. For example, the pull-down list labeled **Scope** can be used to generate the report using only IBM Computers or using all computers in the Notification Database. In this example we are running the report on only IBM computers. Once you have made your selections click **Play** to run the report.

A sample report is shown in Figure 8-32 on page 289.

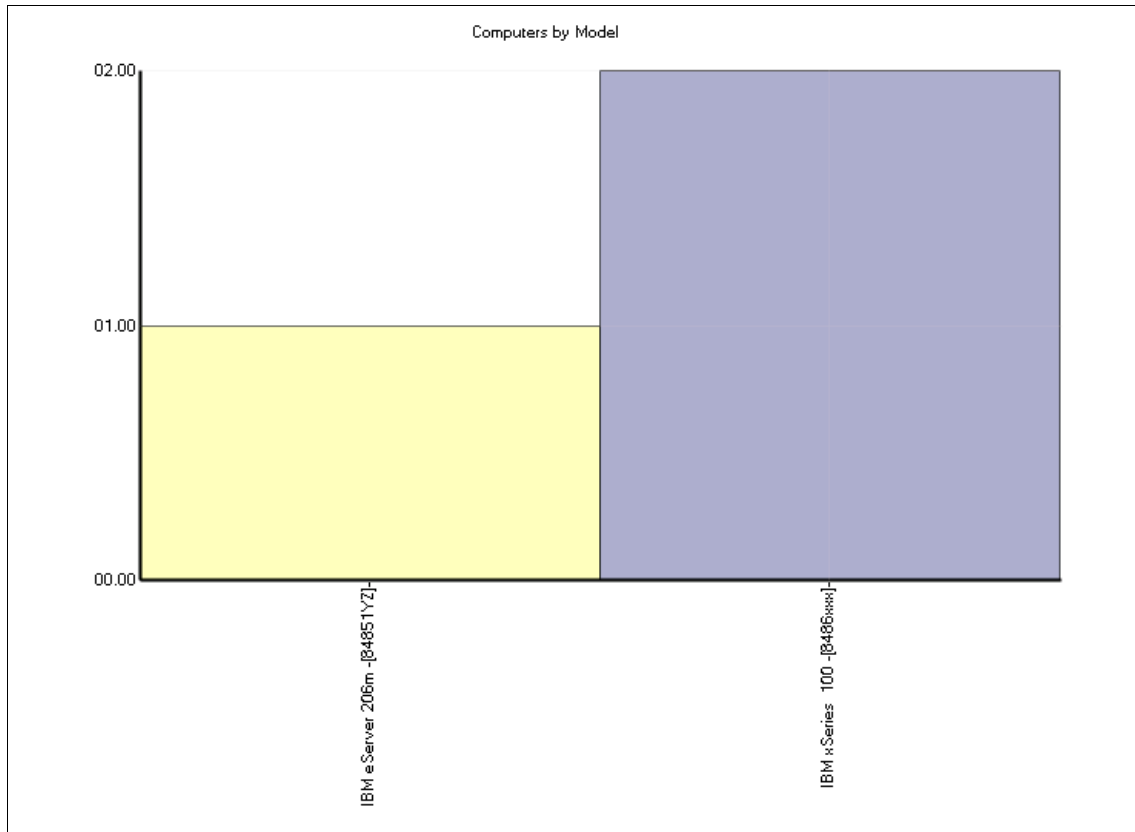


Figure 8-32 A sample report generated for IBM specific hardware from data gathered by Director

8.3 Integration by extension

Altiris has recently released a tool that enables IBM Director to leverage features that have previously been available only in the Deployment Solution Console. This extension for IBM Director is called Deployment Server Extension 1.0 for IBM Director. It is a free download that integrates Deployment Solution functionality into IBM Director without requiring additional software (such as Notification Server, Connector Solution, or the Connector for IBM Director).

Deployment Server Extension 1.0 for IBM Director can be downloaded from:

<http://www.altiris.com/Products/DeploySerExtIBMDir.aspx>

This IBM Director extension integrates IBM Director Server 5.10 with the Deployment Solution Console. The extension adds tasks to launch various Deployment Solutions tools directly from IBM Director Console.

8.3.1 Deployment Server Extension 1.0 for IBM Director

The following features are included in this release of the Deployment Server Extension for IBM Director:

- ▶ Export Director-discovered computers to Deployment Solution

This task lets you export computers that have been discovered in Director to your Deployment Console as virtual computers (for more information about virtual computers and how they can be leveraged see 3.2, “Pre-staging computers for deployment” on page 89). After a computer has been exported to the Deployment Console, you can assign jobs to execute on these computers when they first boot to the Altiris PXE server.

Using this process, you can run scripted operating system installations, capture and deploy disk images, and perform additional pre-boot tasks without installing the Deployment Agent or re-discovering Director-managed computers.

- ▶ Remotely Install the Deployment Agent

This lets you install the Deployment Agent remotely, enabling you to fully manage these computers using Deployment Server. After launching this task, click Help on the Remote Agent Installer window for additional details on the installation process.

- ▶ Launch the Deployment Console

This launches the Deployment Web or Windows Console from the Director interface.

At the time of writing, this feature only worked when the Deployment Console was being installed on the same computer as the IBM Director Server. When we ran this feature on a system where the Deployment Console was not installed we got the message "The eXpress.exe file was not found please make sure Altiris Deployment Solution is properly installed." Altiris development plans were to fix this error in the very near future.

Installing Deployment Server Extension 1.0 for IBM Director

The Deployment Server Extension 1.0 for IBM Director package can be installed only on the system running IBM Director Server or on a system just running IBM Director Console (the latter will require a hotfix).

Before installing Deployment Server Extension for IBM Director make sure the following requirements have been met:

- ▶ Deployment Solution 6.5 or later is installed and running.
- ▶ IBM Director Server 5.10 or later is installed and running on the same subnet as Deployment Solution.
- ▶ If your Deployment Server is located on another computer, you need the NetBIOS or IP address of the computer.
- ▶ If your Deployment Database is located on another computer, you need the NetBIOS or IP address, and the Windows NT or SQL Server authentication credentials. If you select to use Windows NT credentials, the provided account must have rights to the Deployment Database. You must select the correct credential type or the export task will not work.
- ▶ If your Deployment Database is running under a non-default instance of Microsoft SQL Server, select **Another computer**, which is on the SQL Server window of the install process (see Figure 8-35 on page 294) and specify the instance name in the following format:

hostname\instance

To install, run the installation program on your IBM Director server computer.

1. Download and save the Deployment Server Extension 1.0 for IBM Director package onto your IBM Director server computer. The extension can be downloaded from:
<http://www.altiris.com/Products/DeploySerExtIBMDir.aspx>
2. After you have saved and extracted the package run the DS_Director_Extension.msi file on your IBM Director server computer.
3. Click **Next** on the welcome window to begin the install.
4. On the Deployment Server window, you are asked whether the Deployment Server is on this computer or another computer. Select the radio button appropriate to your environment and click **Next** to continue. If you selected **Another computer**, the text box to the right will be enabled. Enter the NetBIOS name or the IP address of your Deployment Server.

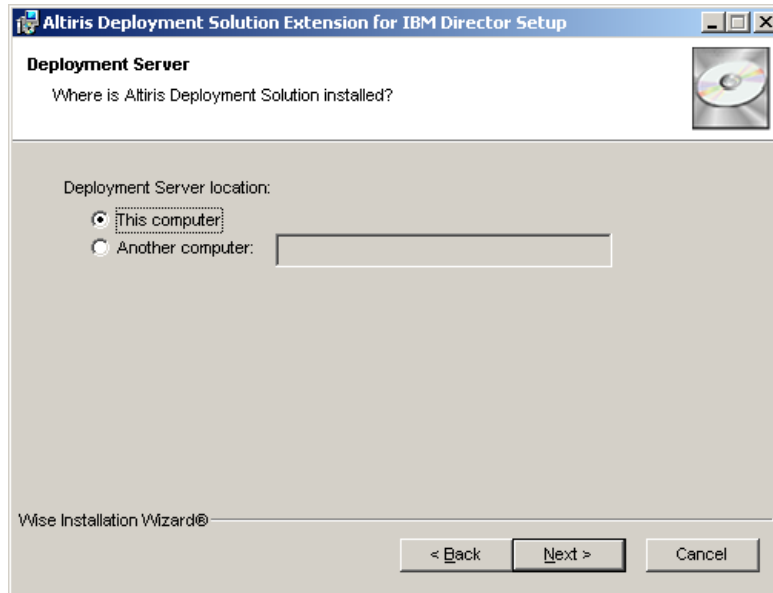


Figure 8-33 The Deployment Server window of the extension installation process

5. On the Console Type window you are asked to select the type of Deployment Console to launch from the IBM Director console. The options are either to launch the Windows console or the Web (Internet Explorer) console. Select the option that is appropriate to your environment and click **Next** to continue.

Note: The console of your choice must be installed and configured for this function to work. For more information about installing additional Deployment Consoles refer to 2.1.5, “Component installation” on page 25.

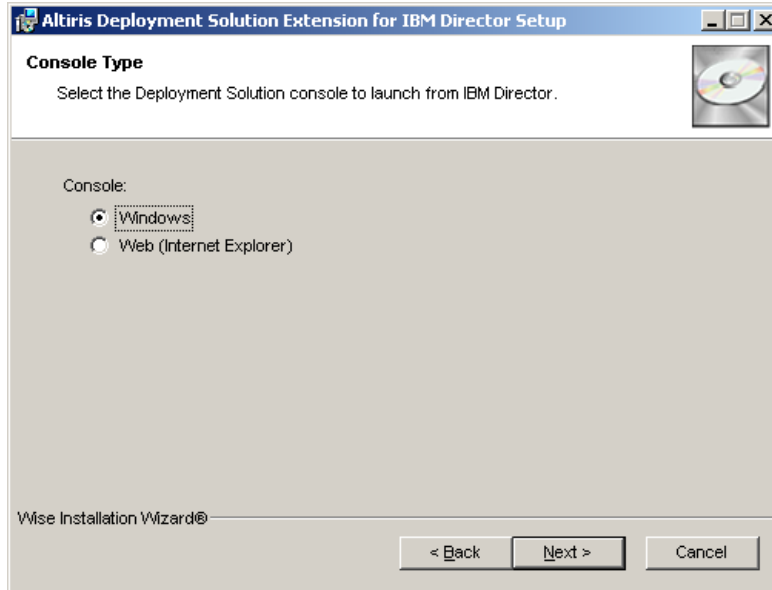


Figure 8-34 The Console Type window of the extension installation process

6. On the SQL Server window you are asked whether the SQL Server is installed on this computer or another computer. Select the radio button appropriate to your environment and click **Next** to continue. If you selected **Another computer**, the text box to the right will be enabled. Enter the NetBIOS name or the IP address of the computer.

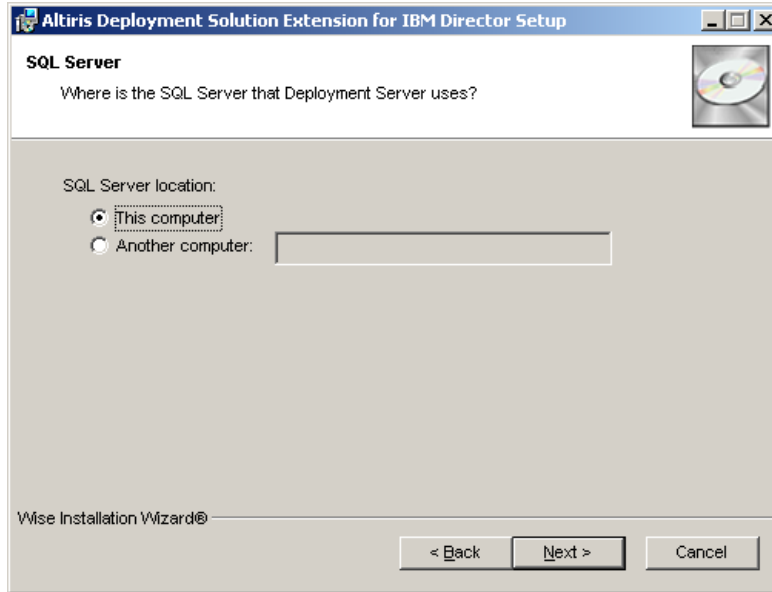


Figure 8-35 The SQL Server window of the extension installation process

7. On the SQL Server Authentication window you have the option to use either Windows NT authentication or SQL Server authentication. If you select **SQL Server authentication**, two text boxes become enabled. Enter the SQL Server user ID in the text box labeled **User ID**, and then enter the password in the text box labeled **Password**. After you have made a selection that is appropriate for your environment, click **Next** to continue.

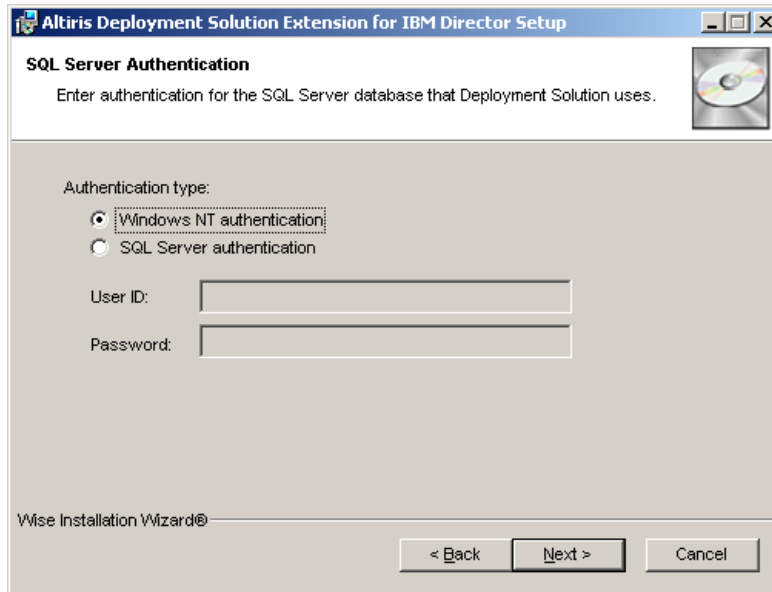


Figure 8-36 The SQL Server Authentication window of the extension installation process

8. When the Installation Summary window loads, click **Next** to begin the installation. When the installation completes, click **Finish** to exit the installer. After the Deployment Server Extension 1.0 for IBM Director has been installed, the new tasks will appear in the Task pane of the Director console.

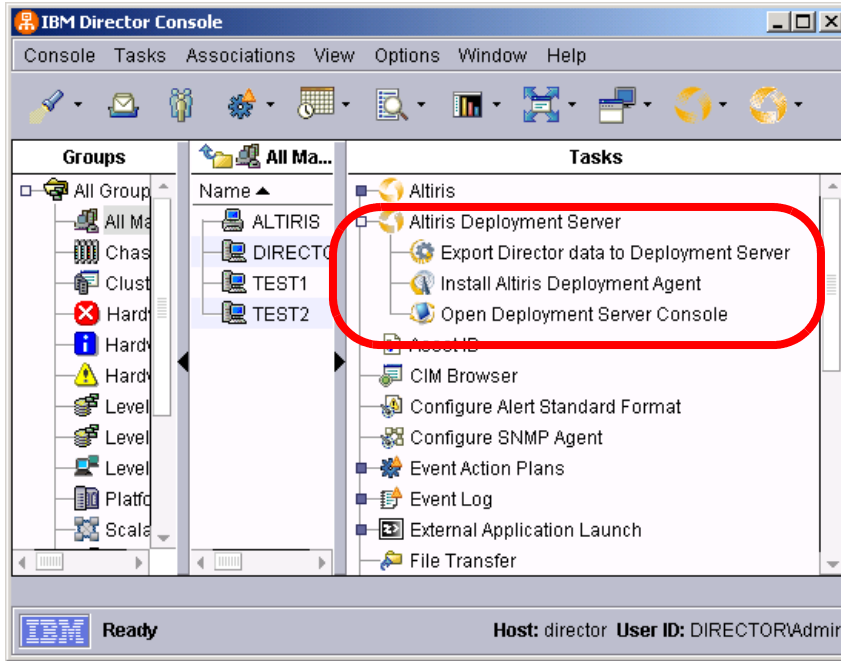


Figure 8-37 The Director console showing the additional tasks

The tasks in the table below are added to the Director console.

Table 8-2 Tasks added to the Director console when the extender has been installed

Component	Description
Export Director data to the Deployment Server	Exports Director-discovered computers to the Deployment Server.
Install Altiris Deployment Agent	Launches the Deployment Agent remote installer tool.
Open Deployment Server Console	Opens the version of the Deployment Console you have installed on your Director server.

The **Install Altiris Deployment Agent** task and the **Open Deployment Server Console** task can both be launched by double-clicking the tasks in the Director console.

The **Export Director data to the Deployment Server** task can be launched by first selecting a computer or group of computers in the Computers pane of the Director console and then dragging the task onto the computer(s).

Exported computers appear in the Computers pane of the Deployment Console, while exported blade chassis and members appear under Physical Devices.

Note: Select **View** → **Show Physical Devices** if these devices are not displayed in the Deployment Console.



Leveraging BladeCenter functionality

This chapter provides instructions on leveraging the functions of IBM BladeCenter with regard to deployment, Rip and Replace, and failover with a hot spare.

The following topics are covered:

- ▶ 9.1, “The Management Module in IBM BladeCenter” on page 300
- ▶ 9.2, “Pre-staging of chassis using virtual bays” on page 301
- ▶ 9.3, “Rip and Replace” on page 313

9.1 The Management Module in IBM BladeCenter

The Management Module installed in the IBM BladeCenter is the management processor for the chassis. It communicates with the service processors in each blade server via an internal management bus. The Management Module supports activities such as Blade server power-on requests, error and event reporting, remote control access, and shared media access. The Management Module also communicates with switch modules, power modules, blower modules, and Blade servers to detect their presence or absence, and any error conditions.

The Management Module stores all event and error information for the BladeCenter. Whether you are configuring a new BladeCenter, modifying settings on an existing BladeCenter, or trying to determine the cause of a problem in the BladeCenter, the Management Module is always the starting point.

The screenshot displays the IBM @server BladeCenter Management Module Web page. The left sidebar contains a navigation menu with categories: Monitors (System Status, Event Log, LEDs, Fuel Gauge, Hardware VPD, Firmware VPD), Blade Tasks (Power/Restart, On Demand, Remote Control, Firmware Update, Configuration, Serial Over LAN), I/O Module Tasks (Admin/Power/Restart, Configuration, Firmware Update), and MM Control (General Settings, Login Profiles, Alerts, Port Assignments, Network Interfaces, Network Protocols). The main content area shows the 'System Status Summary' with a green indicator and the text 'System is operating normally. All monitored parameters are OK.' Below this, there are links for 'Blade Servers', 'I/O Modules', 'Management Modules', 'Power Modules', 'Blowers', and 'Front Panel'. The 'Blade Servers' section includes a table with columns for Bay, Status, Name, Pwr, Owner** (KVM, MT*), and Network (Onboard, Card). The table shows two servers, both with green status indicators.

Bay	Status	Name	Pwr	Owner**		Network	
				KVM	MT*	Onboard	Card
1	●	SN#ZJ1S225BV4W8	Off	X		Eth	Fib ...
2	●	SN#711S725RV4XM	Off			Eth	Fib ...

Figure 9-1 The IBM @server BladeCenter Management Module Web page


The Management Module communicates with Blade computers within BladeCenter via an internal management network. This allows the following tasks to be performed:

- ▶ Start, shutdown, or restart of Blade servers, switch modules, Fibre Channel modules, or management modules from anywhere on the network via a Web browser
- ▶ Viewing the status of all Blade servers within the BladeCenter
- ▶ Viewing the Universally Unique Identifiers (UUIDs) of all devices in the BladeCenter
- ▶ Viewing the serial numbers and FRU numbers of all devices in the BladeCenter
- ▶ Viewing BIOS and firmware levels of all devices in the BladeCenter and update them if needed
- ▶ Access to each Blade computer via remote control with shared media tray access
- ▶ Configuration of Blade policy settings
- ▶ Configuration of the boot sequence of each Blade computer
- ▶ Configuration of Management Module settings

All these functions are very useful during deployment process using Altiris Deployment Solution. For more details on the capabilities and use of the Management Module, see the IBM Redbook *IBM @server xSeries and BladeCenter Server Management*, SG24-6495.

9.2 Pre-staging of chassis using virtual bays

To maximize the manageability of Blade servers, the Deployment Console provides a physical devices view that displays Blade computers in a rack/enclosure/bay hierarchy. By default, physical devices view is not enabled on the Deployment Console.

To enable the physical devices view click **View** → **Show Physical Devices** on the main menu of the Deployment Console. One of three icons  appears as physical representations to support management of different levels of the BladeCenter structure.

When physical devices view has been enabled, Blade servers and BladeCenter chassis will be displayed as shown in Figure 9-2 on page 302.

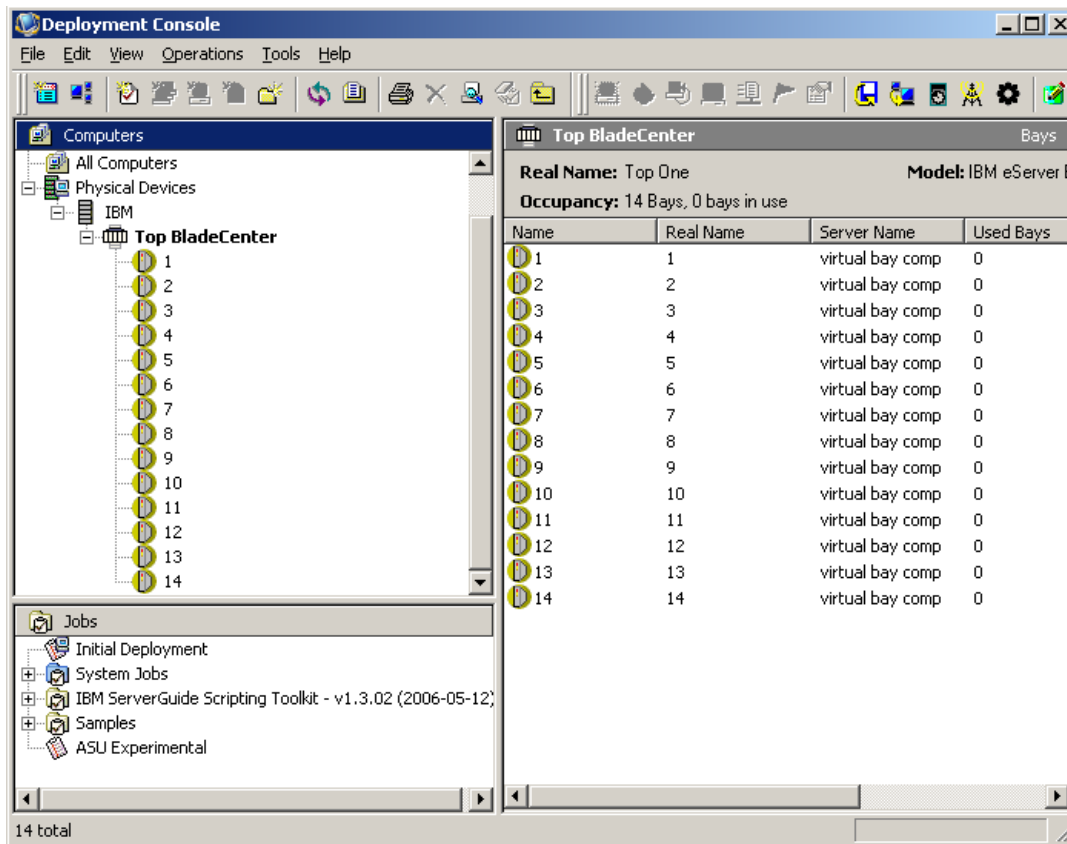



Figure 9-2 The Deployment Console with physical devices view enabled

9.2.1 Virtual bays

Deployment Solution has a virtual bay feature that allows you to pre-assign deployment jobs to racks, enclosures, or specific Blade servers in BladeCenter bays that are not currently known by the Deployment Server. Any IBM Blade server can have predefined deployment jobs and configuration tasks associated with it to execute automatically upon contacting the Deployment Server. A virtual Blade server object icon will have a yellow background  to differentiate it from a currently managed system. The virtual rack, enclosure, bay icons will change from virtual icons to managed system icons as Blade servers are inserted and identified by Deployment Solution.

When new Blade servers are identified in a bay that has not been used previously, then both initial deployment and virtual bays features can be set up to automatically run configuration tasks and deploy jobs.

This feature enables you to prestage Blade servers before they even arrive at your location.

Note: For IBM blade servers in physical devices view, the rack name is always IBM. All subordinate Enclosures are identified by the chassis UUIDs under IBM rack name and bays are identified by numbers as shown in Figure 9-2 on page 302.

To create a new virtual bay:

1. On the Deployment Console, right-click the **Physical Devices** icon in the Computers pane and click **New Virtual Bay** from the pop-up menu.

The Create Virtual Bays window appears, as shown in Figure 9-3.

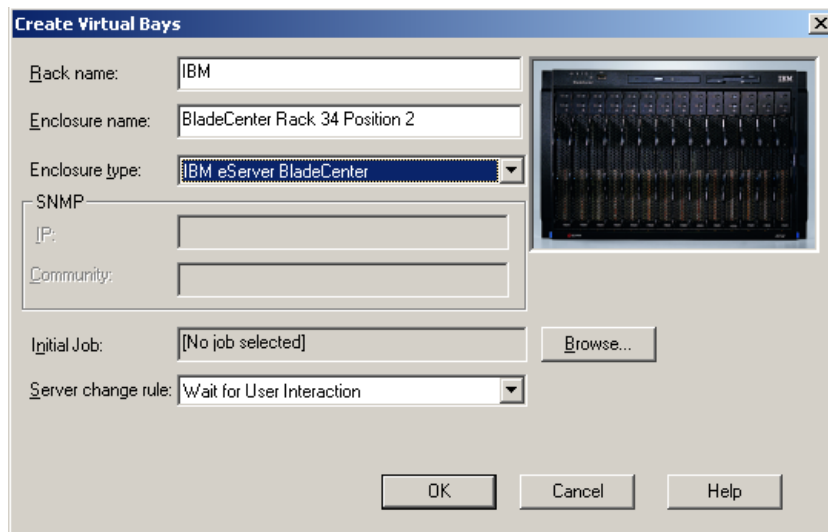


Figure 9-3 The Create Virtual Bays window

2. In the field Rack Name, enter IBM as the rack name.

Note: For IBM Blade servers in the physical devices view, the Rack name will always be IBM. All subordinate Enclosures are identified with custom names under the IBM Rack name and Bays are identified by number. For example:

```
IBM
<EnclosureName>
<BayNumber>
```

3. In the field Enclosure name, enter an enclosure name according to your naming conventions.
4. In the pull-down list for Enclosure type, select **IBM eServer BladeCenter** or **IBM eServer BladeCenter T** depending on the type of enclosure you are pre staging. A picture of a fully populated BladeCenter chassis will appear on the right side of the window.
5. When an IBM Blade server is inserted into a BladeCenter chassis bay that has been preconfigured but not previously known by the Deployment Server to have existed in that bay, an initial job can be run. If you want to perform an initial job click **Browse** next to the Initial job field. A window appears showing predefined jobs as shown in Figure 9-4. Select the job you want to run and click **OK**.

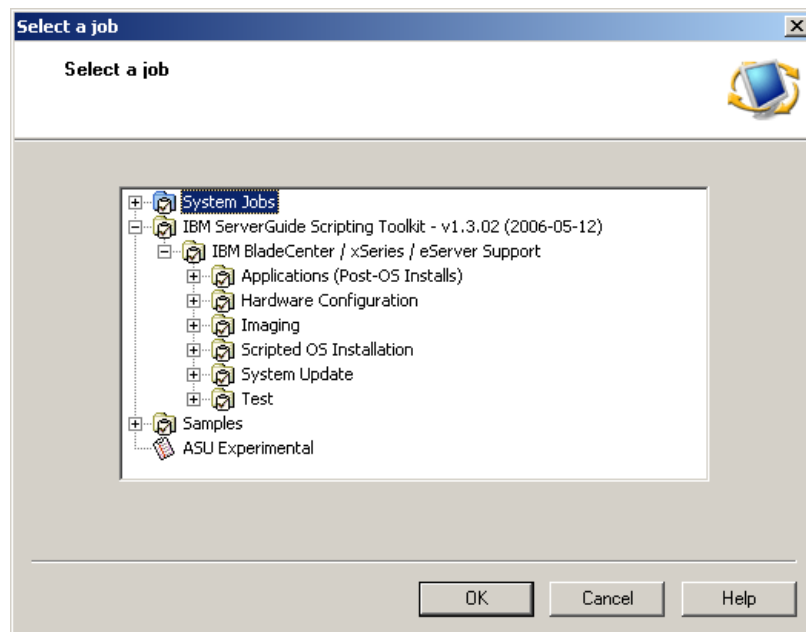


Figure 9-4 Select a predefined job to run

6. In the pull-down list for **Server change rule**, you can select what you want to do when a new Blade computer is installed. The options are listed in Table 9-1 on page 305 and shown in Figure 9-5 on page 305.

Table 9-1 Server change rules

Rule	Action
Re-Deploy Computer	Restore a Blade computer using deployment tasks and configuration settings saved from the previous Blade computer in the bay. This lets you replace new Blades in the bay and automatically run deployment tasks from its deployment history. All deployment tasks in the bay's history will be executed starting from the last Distributing a Disk Image task or Scripted OS Install task, or from any script (in a Run Script task) with this command: rem deployment start .
Run Predefined Job	The Blade computer will process any specified job. Select a job to run automatically when a new server is detected in the bay.
Ignore the Change	This option lets you move Blade computers to different bays without automatically running jobs. The Blade computer placed in the bay is not identified as a new computer and no jobs are initiated. If the Blade existed in a previous bay, the history and parameters for the Blade are moved or associated with the new bay. If the Blade is a new computer (never before identified), then the established process for managing new computers will be executed.
Wait for User Interaction	(default) No job or tasks are performed (the Deployment Agent on the Blade computer is instructed to wait). The icon on the console changes to reflect that the computer is waiting.

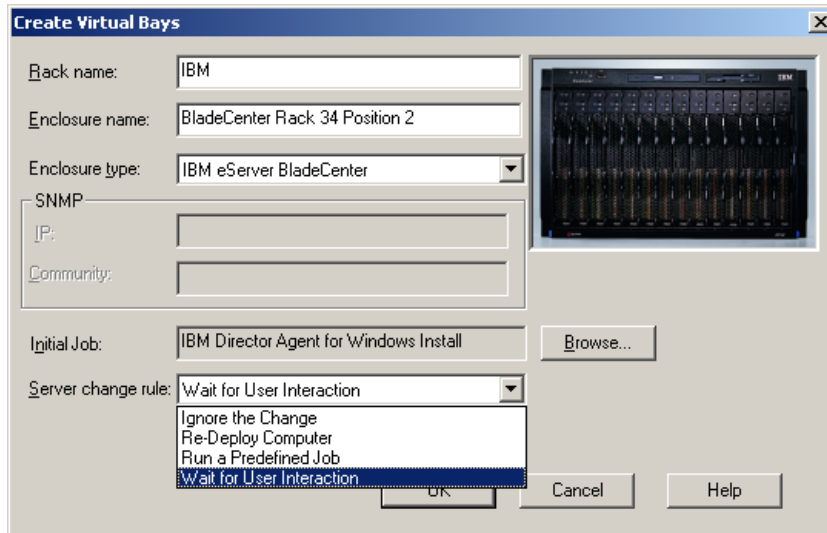


Figure 9-5 Server Change rules

7. Click **OK** when you have made your selections. The Computer Configuration Properties window appears.

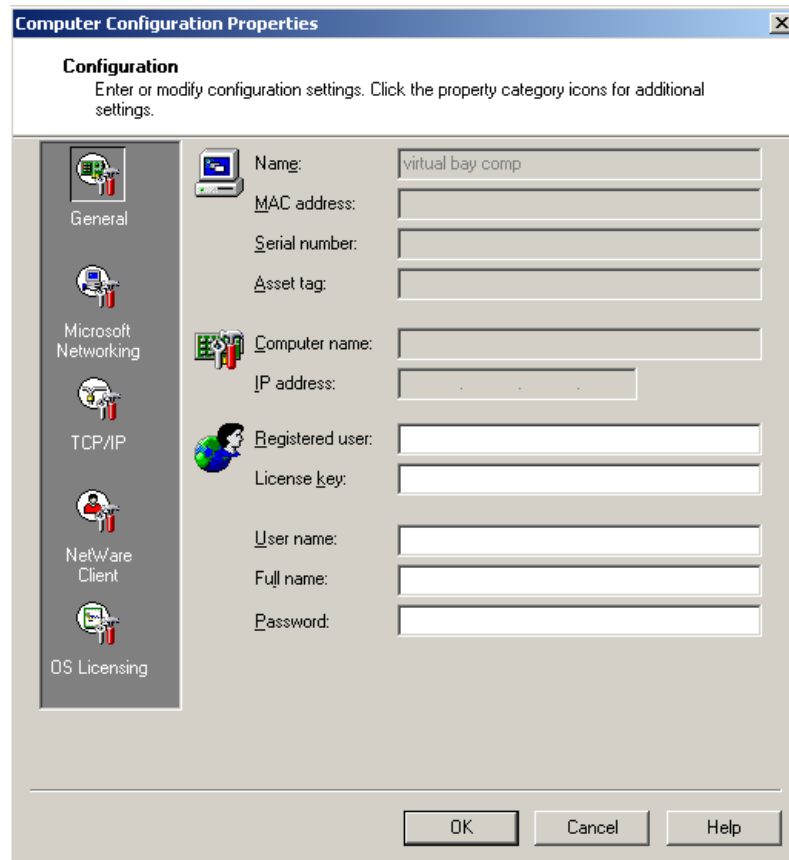


Figure 9-6 The Computer Configuration Properties window

8. If you want to fill out additional information, click the various icons on the left side of the Computer Configuration Properties window and fill in the fields with information specific to your environment. This step is optional. Click **OK** to complete the setup of virtual bays.

Leveraging the Computer Configuration Properties window

The Computer Configuration Properties window, shown in Figure 9-6, is a valuable tool for prestaging Blade computers. This section will cover some of the value-add features that reduce time-to-production when your new BladeCenter chassis and Blade computers arrive at your location.

The Computer Configuration Properties window will be displayed when you add a new virtual enclosure as described in the previous section, or by right-clicking an existing enclosure and selecting **Configure** from the pop-up menu.

The Blade server's NetBIOS name can be pre configured from within the Computer Configuration Properties window. To do so, follow the steps outlined below:

1. Click the **Microsoft Networking** icon on the left side of the Computer Configuration Properties window and then click **Define Range**.
2. When the Computer Name Range window appears, using your company's naming conventions enter a meaningful name for the Blade computer in the **Fixed text** text box. The information you enter here will be appended to the beginning of each new Blade computer's NetBIOS name.
3. The **Range start text box** is used to append numeric information to the end of the Blade Computer's NetBIOS name. The number will increment for each Blade computer so no computers get the same NetBIOS name. Enter a number and make sure the checkbox labeled **Append** is checked. The Result field displays how the Blade computers' NetBIOS name will look.

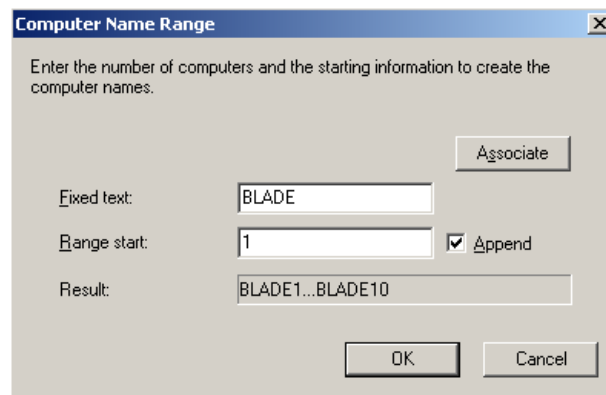


Figure 9-7 The Computer Name Range window

4. Click **Associate** in the Computer Name Range window to bind the virtual bays with associated names. When the Associate button is clicked, the Associate Range Configuration Data window is shown (Figure 9-8 on page 308).

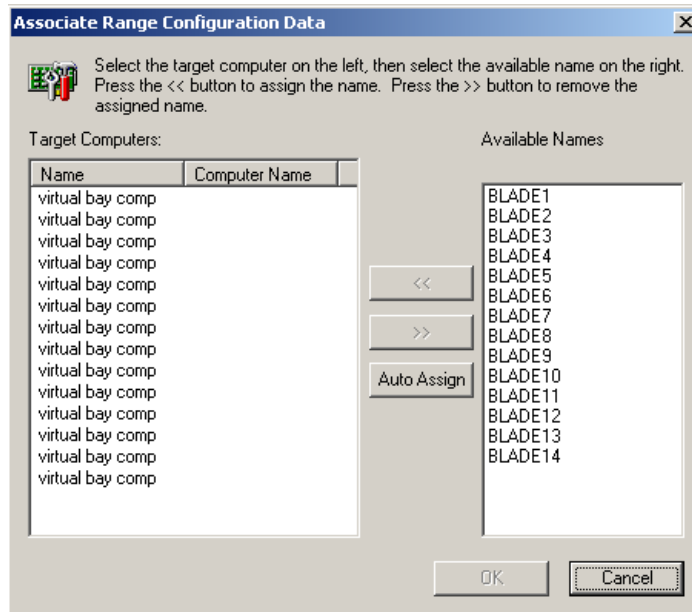


Figure 9-8 The Associate Range Configuration Data window

5. To automatically associate the virtual bays with a pre-configured NetBIOS names click **Auto Assign** in the middle of the window. This associates the virtual bays in the left pane with the computer NetBIOS names in the right pane.

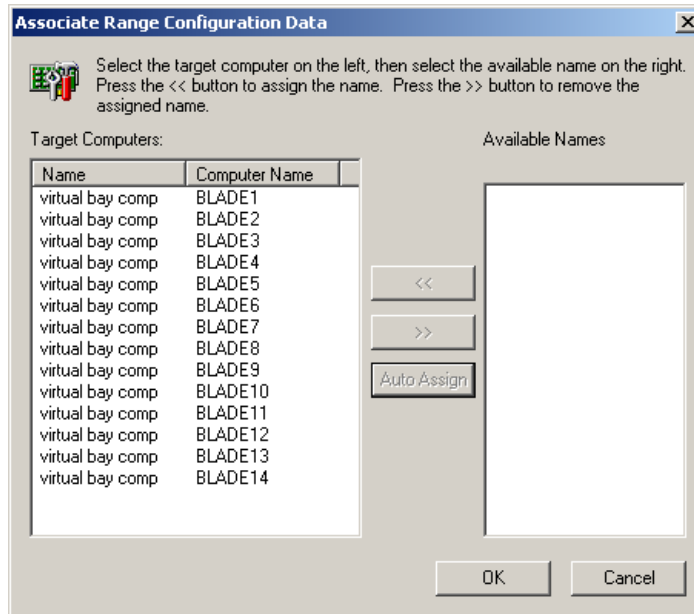
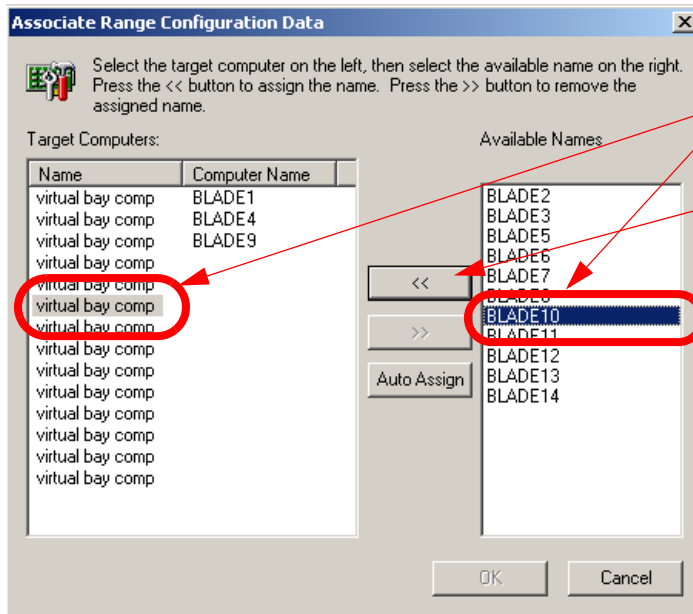


Figure 9-9 The Associate Range Configuration Data after auto assigning the computer names

6. If you would rather assign specific names to specific virtual bays, you can do so by selecting an individual bay in the left pane and then selecting an individual computer name in the right pane and then clicking the << button.



1. Start by selecting a virtual bay and a computer name.
2. Then click the << button to assign the name to the virtual bay.

Figure 9-10 The Associate Range Configuration Data window after assigning specific names

3. When you have finished assigning names click **OK** to return to the Computer Name Range window. Click **OK** to return to Microsoft Networking window.

Another useful feature is the ability to predefine a range of IP addresses to use as the Blade computers are installed and become active.

To define a range of IP addresses follow these steps:

1. Assuming that you have not closed the Computer Configuration Properties window shown in Figure 9-6 on page 306, click the **TCP/IP** icon on the left side of the window. If you have closed the window, you can display it by right-clicking an existing enclosure and selecting **Configure** from the pop-up menu.

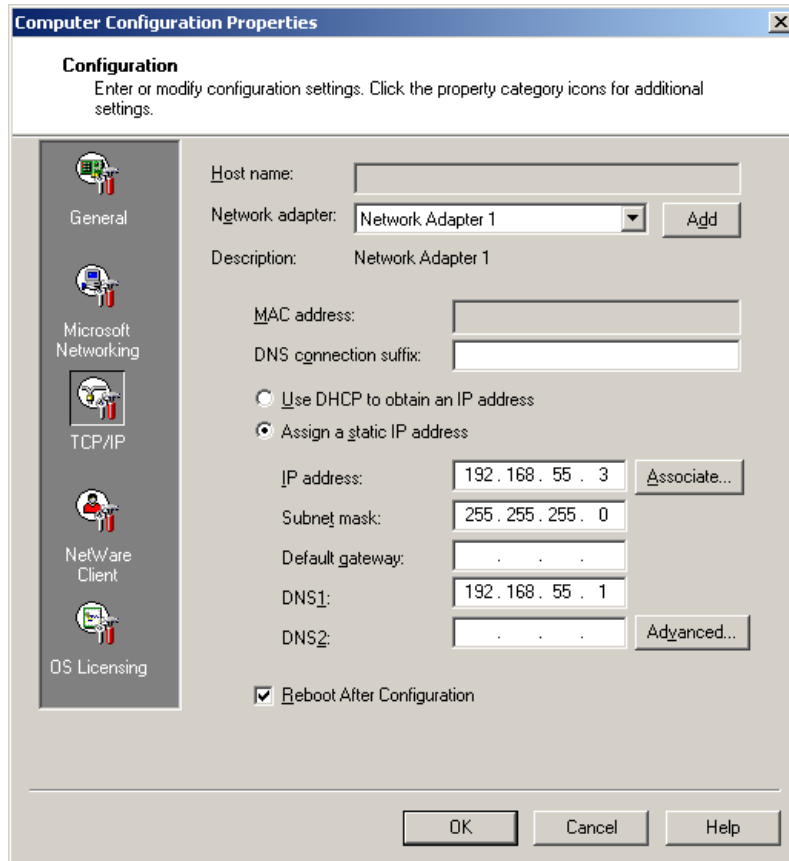


Figure 9-11 The Computer Configuration Properties window with the TCP/IP tab shown

2. Select **Assign a static IP address** and enter a starting IP address in the **IP Address** field. Fill out the next four fields (Subnet mask, Default gateway, DNS1, and DNS2) with information pertinent to your environment.

Note: The information shown on the form was entered to match our test environment. You would fill in the fields with information to match your environment.

3. To associate the IP addresses to the virtual bays, click **Associate** in the middle-right side of the window. The Associate Range Configuration window opens, displaying a list of IP addresses using the IP address you entered as the starting address and incrementing by one for each virtual bay.

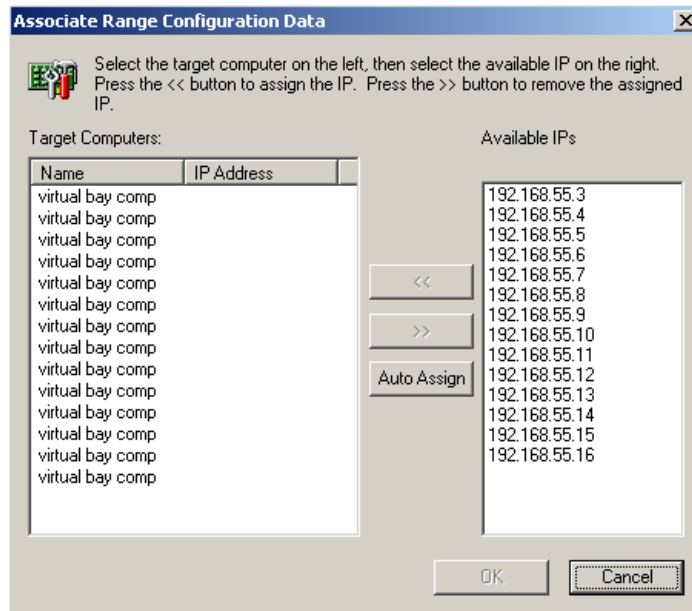


Figure 9-12 The Associate Range Configuration Data window showing a list of IP addresses

4. Assign IP addresses to virtual bays in the same manner as you assigned NetBIOS names on page 307.
5. When you have finished assigning IP addresses, click **OK** to return to the Computer Configuration Properties window. Click **OK** to close the Computer Configuration Properties window.

Assuming the Management Module, Ethernet Switch Modules and optional Fibre Channel Switch Modules are configured and connected to physical network and SAN fabric, you are ready to deploy your new blade servers.

When the new Blade servers arrive, are installed in the BladeCenter chassis, powered on, and have contacted the Deployment Server, the Deployment Server will recognize the Blade bay number and associate it with the Initial Job and Server Change Rule you defined above.

When deployment jobs are completed, the new Blade will appear in Computer pane with the NetBIOS name and static IP address you defined.

9.3 Rip and Replace

Using Altiris Deployment Solution, you can employ “Rip and Replace” technology that lets you replace an existing Blade with a new Blade and automatically configure and deploy the new Blade using the deployment history of the Blade it replaced. This method is used to quickly get a failed server back online.

Rip and Replace is a native functionality of Deployment Solution for Blade servers. It offers four Server Change Rules to be executed on the Blade when the replacement occurs. To access the Server Change Rules for each Blade, double-click the Blade icon in the Computers pane of the Deployment Console (if physical devices view has been enabled) as shown in Figure 9-13.

To display the physical devices view, from the Deployment Console, click the **View → Show Physical Devices**.

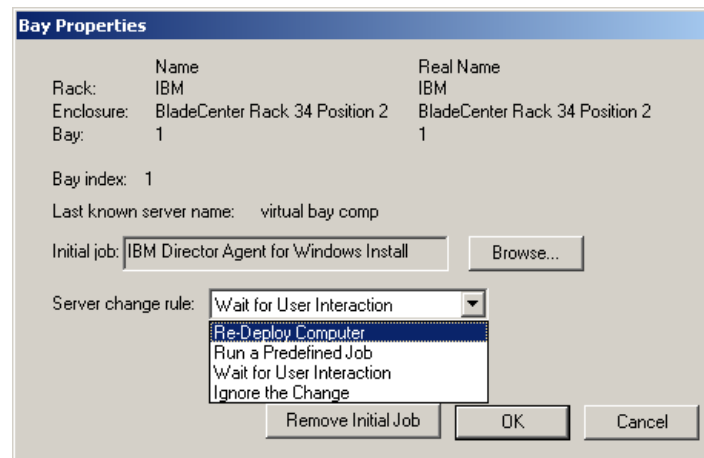


Figure 9-13 Server Change Rules

For information regarding each Server Change rule see Table 9-1 on page 305.

9.3.1 Rip and Replace process flow

The Rip and Replace process flow is as follows:

1. Blade server is removed from slot/bay.
2. New or replacement Blade is inserted into the same slot/bay.
3. New or replacement Blade is powered on manually or by using Wake-On-LAN.

4. The PXE server checks its local cache and does not recognize the “new” Blade as a managed computer.
5. The PXE server requests any pending job assignments from the Deployment Server.
6. The Deployment Server determines the blade is “new” and executes the Server Change Rule that was configured for that slot/bay.

For example: If the Re-Deploy Computer Server Change Rule was configured, the Deployment Server would replay the bay’s deployment history from the last Distribute Image task forward.

9.3.2 Some considerations

Although Rip and Replace is a valuable feature of Deployment Solution, there are a few considerations to keep in mind.

- ▶ Rip and Replace technology is a fail-safe feature from Altiris. It is not a backup solution. You still need to establish a routine backup policy to backup your data. Actual data are not captured/deployed. When your replacement Blade computer is back online, you will need to restore your data from backup.
- ▶ Rip and Replace replays only the deployment history of the previous Blade server. Any software installations, including hot fixes and security patches, that are not in the deployment history (that is, applications that were not deployed using Deployment Solution) will not be restored. You need to verify all software packages, including hot fixes and security patches, are installed after deployment has been replayed.
- ▶ Test this feature to familiarize yourself with the process before using it in a production environment or operations.

Abbreviations and acronyms

ACPI	advanced control and power interface	LAN	local area network
AMD	Advanced Micro Devices	LUN	logical unit number
BIOS	basic input output system	MAC	media access control
CD	compact disk	MB	megabyte
CD-ROM	compact disc read only memory	MBR	Master Boot Record
CMOS	complementary metal oxide semiconductor	MIB	management information base
CSV	comma separated variable	MIME	Multipurpose Internet Mail Extensions
DHCP	Dynamic Host Configuration Protocol	MM	Management Module
DOS	disk operating system	MPCLI	management processor command line interface
FAT	file allocation table	MS	Microsoft
FIRM	File System Independent Resource Management	MSI	Microsoft Installer
FRU	field replacable unit	MTFTP	Multicast Trivial File Transfer Protocol
FTP	file transfer protocol	NFS	network file system
GB	gigabyte	NIC	network interface card
HAL	hardware abstraction layer	NTFS	NT File System
HBA	host bus adapter	OS	operating system
HTTP	Hypertext Transfer Protocol	PC	personal computer
I/O	input/output	PE	Preinstallation Environment
IBM	International Business Machines Corporation	POST	power on self test
ID	identifier	PRAID	Policy-based RAID
IDE	integrated drive electronics	PXE	Pre-boot-execution
IIS	Internet Information Server	RAID	redundant array of independent disks
IP	Internet Protocol	RAM	random access memory
ISO	International Organization for Standardization	RMON	Remote Monitoring
IT	information technology	ROM	read-only memory
ITSO	International Technical Support Organization	RPM	Red Hat Package Manager
		RSA	Remote Supervisor Adapter
		SAN	storage area network

SAS	Serial Attached SCSI
SCSI	small computer system interface
SGTK	ServerGuide Scripting Toolkit
SID	system ID
SL	SlimLine
SMBIOS	system management BIOS
SNMP	Simple Network Management Protocol
SOL	Serial over LAN
SQL	structured query language
SSTK	ServerGuide Scripting Toolkit
TCP/IP	Transmission Control Protocol/Internet Protocol
UNC	universal naming convention
UNDI	Universal Network Driver Interface
URL	Uniform Resource Locator
USB	universal serial bus
UUID	Universally Unique Identifier
UXCD	UpdateXpress CD
VM	virtual machine
WWN	World Wide Name

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

IBM Redbooks

For information on ordering these publications, see “How to get IBM Redbooks” on page 319. Note that some of the documents referenced here may be available in softcopy only.

- ▶ *Implementing IBM Director 5.10*, SG24-6188
- ▶ *IBM @server xSeries and BladeCenter Server Management*, SG24-6495

Other publications

These publications are also relevant as further information sources:

- ▶ *Altiris Deployment Solution 6.5 Reference Guide*, available from:
http://www.altiris.com/upload/deployment_002.pdf
- ▶ *Altiris RapiDeploy 6.1 Product Guide*, available from:
<http://www.altiris.com/upload/rapideployguide.pdf>
- ▶ *Altiris Deployment Solution 6.5 Release Notes*
<http://kb.altiris.com/article.asp?article=21759&p=3>
<http://www.altiris.com/Support/Documentation.aspx>

Online resources

These Web sites and URLs are also relevant as further information sources:

IBM resources

- ▶ IBM Support home
<http://www.ibm.com/support>

- ▶ IBM Director
http://www.ibm.com/servers/eserver/xseries/systems_management/ibm_director/
- ▶ UpdateXpress
http://www.ibm.com/servers/eserver/xseries/systems_management/ibm_director/extensions/xpress.html
- ▶ ServerGuide
http://www.ibm.com/servers/eserver/xseries/systems_management/serverguide.html
- ▶ ServerGuide Scripting Toolkit
http://www.ibm.com/servers/eserver/xseries/systems_management/sgstk.html
- ▶ UpdateXpress Server
http://www.ibm.com/servers/eserver/xseries/systems_management/uxsrv.html
- ▶ Management Processor Command Line Interface (MPCLI)
<http://www.pc.ibm.com/support?page=MIGR-54216>
- ▶ RETAIN tip: ServerGuide scripting toolkit errors loading Altiris Binary
<http://www.pc.ibm.com/support?page=MIGR-62782>

Altiris resources

- ▶ Altiris downloads
<http://www.altiris.com/download.aspx>
- ▶ Altiris Connector for IBM Director
<http://altiris.com/Products/ConnectorforIBMDirector.aspx>
- ▶ Product documentation
<http://www.altiris.com/Support/Documentation.aspx>
- ▶ Product updates
<http://www.altiris.com/support/updates/>
- ▶ Deployment Solution Reference Guide
http://www.altiris.com/upload/deployment_002.pdf
- ▶ RapidDeploy Product Guide
<http://www.altiris.com/upload/rapiddeployguide.pdf>

Microsoft resources

- ▶ A PXE client computer is slow to start when you deploy Windows PE from a Windows Server 2003-based RIS server
<http://support.microsoft.com/kb/906425>
- ▶ Customizing SQL/MSDE unattended installation files
<http://support.microsoft.com/kb/233312>
- ▶ Command-line switches for Microsoft software update packages
<http://support.microsoft.com/kb/824687>
- ▶ Unattend.txt File Parameters
<http://www.microsoft.com/technet/prodtechnol/Windows2000Pro/deploy/unattend/sp1ch01.msp>

Others

- ▶ Syslinux downloads
<http://www.kernel.org/pub/linux/utils/boot/syslinux>
- ▶ Red Hat product documentation
<http://www.redhat.com/docs/manuals/linux/>
- ▶ VMware product documentation
<http://www.vmware.com/support/pubs/>

How to get IBM Redbooks

You can search for, view, or download Redbooks, Redpapers, Hints and Tips, draft publications and Additional materials, as well as order hardcopy Redbooks or CD-ROMs, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Index

A

- AClient
- ACPI support 202
- activation keys 27
- Active Directory 11
- ADLagent 161
- Agent 11
- Altiris Deployment Solution
 - See Deployment Solution
- AMD K6 processors 101
- answer file 139
- Application Management 4
- applications 229–248
- Asset Tag 76
- AuditExpress 5
- automation 58
- automation partitions 63

B

- backup 75
- best practices 75–77
- BIOS
 - settings 106
 - updates 104
- BladeCenter 299–314
 - Rip and Replace 313
 - virtual bays 302
- BladeCenter Management Module 69
- Boot Disk Creator 185, 226
- boot from SAN 129
- boot media 63
- BootWorks 68
- broadcast 68

C

- CMOS settings 106
- computer name 77
- console 10
 - physical devices view 301
 - Show Physical Devices 301
- CSV file 93

D

- database 10
- default job 80
- Deployment Agent 46
 - Access tab 49
 - Automatically Add to a Group 55
 - boot disk prompt 54
 - connect to server 48
 - connection to server 23
 - default settings 48
 - delay 53
 - encryption 50
 - Linux installation 58
 - Log File tab 51
 - manual install 57
 - password protect 51
 - Proxy tab 52
 - remote control 49
 - remote install 47
 - Security tab 50
 - settings 48
 - Startup/Shutdown tab 53
 - Sysprep 54
 - time sync 53
 - timeout 49
 - tray icon 51
 - user response 49
 - Windows install 47
- Deployment Console 10
 - ServerGuide Scripting Toolkit 33
- Deployment Database 80
- Deployment Share 10
- Deployment Solution
 - activation keys 27
 - Active Directory 11
 - automation partitions 63
 - boot media 63
 - compare to Deployment Server 2
 - component installation 12, 25
 - components 10
 - connection to server 23
 - custom installation 12, 18
 - database 13, 20
 - Discover Deployment Server 23

- discovery utility 69
- disk space 12
- DOS 60
- drive letter 99
- Fedora Linux 61
- Fibre Channel 129
- Ghost comparison 168
- hardware support 12
- IBM Director discovery utility 69
- image-based deployment 167–227
- Initial Deployment 80–89
- installation 9–77
- introduction 2
- IP address 19
- issues 99
- job troubleshooting 96
- license 15
- license keys 27
- memory 12
- MSDE 13
- MS-DOS 16
- networking 11
- operating system support 11
- power control 70
- PRAID utility 120
- Pre-Boot Operating System window 16
- pre-boot operating systems 60
- prerequisites 11
- pre-staging 89–93
- primary lookup key 76
- PXE 62, 64–69
- PXE Server 14
- RAID configuration 120
- remote installation 19
- requirements 11
- Rip and Replace 313
- script-based deployment 139–166
- Service Processor Discovery Utility 69
- Show Physical Devices 301
- simple install 13
- simple installation 12
- Solaris support 99
- SQL Server 13, 20
- Sysprep 17, 193–202
- TCP/IP 11
- troubleshooting 99
- UpdateXpress 114
- virtual bays 302
- Windows PE 61, 221

- DHCP Server 11
- discovery utility 69
- disposal 135
- DOS 60
- drive letter 99

E

- Error 1326 99
- Error 16 100
- Error 1722 30
- ESX Server 157
- Ethernet ports 75
- Event Notification policies 4

F

- Fedora Linux 61
- Fibre Channel configuration 129
- FIRM 209, 218
- forwarding packets 68

G

- Ghost 168

H

- HAL 202
- hardware support 12
- hardware-independent images 202–219
 - device drivers 208
 - FIRM 218
 - overall process 203
 - registry changes 212
 - ServerGuide 208
 - Sysprep 204
 - Windows PE 220
- HBA 129
- hotfix deployment 239
- hotfixes 26

I

- IBM Director Agent 230
- IBM Director discovery utility 69
- icons 302
- image-based deployment 167–227
 - capture 170
 - deploy 176
 - hardware-independent images 202–219
 - job wizard 177

- multicast 182
- New Job Wizard 174
- partitions 179
- RapiDeploy 167, 180
- starting capture 173
- Sysprep 178
- unicast 182
- Windows capture 171
- Initial Deployment 80–89
 - active agent 84
 - Advanced Configuration window 83
 - Advanced tab 88
 - batch mode 84
 - configuration tab 80
 - create new job 85
 - existing job 87
 - Jobs tab 85
 - minimum clients 84
 - New Job Wizard 82
 - PXE 88
 - timeout 84
- installation 9–77
 - applications 229–248
 - component install 25
 - custom install 18
 - Deployment Agent 46
 - Discovery Utility 70
 - IBM Director Agent 230
 - MPCLI 71
 - remote install 19
 - ServerGuide Scripting Toolkit 29
 - simple install 13
 - SQL Server 2000 235
 - Sysprep 194
- Intel UNDI driver 185
- introduction 1
- Inventory Solution 4

J

jobs

- add task menu 87
- BIOS settings 106
- BIOS update 105
- CMOS settings 106
- create an image 174
- create new 85
- default 80
- deploy image 176

- description 86
- failures 97
- Fibre Channel 129
- image creation 174
- image deploy 176
- Initial Deployment 80
- linking multiple jobs 93
- Linux Scripted Install 154
- log 98
- name 86
- New Job Wizard 82
- RAID configuration 125
- scripted OS install 140
- ServeRAID firmware 108
- SQL 2000 Unattended Install 237
- status 98
- super job 94
- task 87
- tasks 93
- troubleshooting 96
- UpdateXpress 115
- Windows Scripted Install 145

K

- keys 27
- kickstart file 139

L

- license 15
- license keys 27

M

- MAC Address 76
- Management Module 300
- manual pre-staging 90
- mass storage device drivers 100
- Microsoft IIS 24, 150
- Monitor Solution 5
- MPCLI 70
- MSDE 2000 13
- MTFTP 11, 68
- multicast 68, 182

N

- name 77
- NetBIOS name 77
- Notification Server 2

O

operating system support 11

P

package deployment 239

Package Servers 3

patch deployment 239

Patch Management Solution 4

policies

Event Notification 4

PRAID policies 120

power control 70

PRAID utility 120

pre-boot environment 58

pre-boot operating systems 60

pre-staging 89–93

primary lookup key 76

profiles 82

PXE 62, 64–69

additional servers 69

connecting 67

Ethernet ports used 75

forwarding packets 68

Initial Deployment 88

menu limitations 101

network boot 66

network layout 66

Serial over LAN issues 76

subnets 68

PXE Server 11, 21, 65

Q

QLogic 134

R

RAID configuration 120

RapiDeploy 64, 167, 182

Real Time System Manager Solution 5

Recovery Solution 5

Red Hat install 155

Redbooks Web site 319

Contact us xii

Remote Supervisor Adapter II 69

RemoteUX 113

Rip and Replace 313

S

script-based deployment 139–166

AdminPassword 144

answer file 142

compare with image-based 140

Components 145

ComputerName 144

ComputerType 144

ESX Server 157

FullName 144

HAL 144

kickstart file 151

Linux 150

mass storage drivers 143

Microsoft IIS 150

MIME Types 150

partition size 143

prerequisites 142

ProductID 144

steps 141

VMware ESX Server 157

scrub3 utility 136

secure disposal 135

SeeDeployment Agent

Serial Number 76

Serial over LAN 76

Server Management Suite 4

ServeRAID firmware 107

ServerGuide 208

ServerGuide Scripting Toolkit 28

application files 36

BIOS settings 106

BIOS updates 104

CMOS settings 106

Configuration Utility 35

device driver files 40

Error 1722 30

IBM Director Agent deployment 230

integration 32

introduction 6

manual integration 34

operating system installation files 42

operating system utility files 44

PRAID utility 120

RAID configuration 120

Red Hat support 43

script-based deployment 140

ServeRAID firmware 107

source tree 35

- SUSE Linux support 43
 - syslinux 44
- Windows Scripted Install 145
- Windows support 43
- Service Processor Discovery Utility 69
- share 10
- Show Physical Devices 301
- SIDgen utility 54
- Site Monitor Solution 5
- Software Delivery Solution 4
- Solaris support 99
- source tree 35
- SQL Server 2000 13, 20
 - deployment 235
- subnets 68
- super job 94
- Symantec Ghost Solutions Suite 168
- Sysprep 17, 54, 193–202
 - benefits 193
 - deployment using 201
 - global settings 196
 - hardware-independent images 204
 - installation 194
 - integrating with Deployment Solution 194
 - product keys 199
 - SourceDisksNames 206
 - SysprepMassStorage section 204
 - using during image capture 199

- Windows PE 61, 220
 - advantages 220
 - boot disk 220–221
 - Deployment Solution integration 221
 - mass storage drivers 225
 - slow download defect 220
- Wise Packager 242
- Wise Script Toolkit 5
- wizard, new job 82
- wlogevent.exe 234
- WWN 134

T

- tasks 93
- time sync 53

U

- unattended installs 242
- UNDI driver 185
- updates 26
- UpdateXpress 113

V

- virtual computers 89
- VMware ESX Server 157

W

- Wake-on-LAN 52
- Web Console 11, 24
- Web reports 4



Deployment using Altiris on IBM System x and BladeCenter Servers

(0.5" spine)
0.475" <-> 0.875"
250 <-> 459 pages



Deployment using Altiris on IBM System x and BladeCenter Servers



Describes the integration of Altiris products with System x tools

Deploying firmware, operating systems, drivers, and applications

Covers script-based and image-based deployments

Altiris Deployment Solution is an industry leading management product which helps reduce the cost of deploying servers from bare metal and managing them all from a centralized location. Its user interface makes it easy to deploy operating systems and applications, apply custom configurations, and distribute software updates.

Deployment Solution runs in either a virtual or physical server environment and supports deploying Linux, Windows, and ESX Server, as well as virtual machines to an ESX Server system. Deployment Solution also integrates with the IBM ServerGuide Scripting Toolkit to offer custom scripts for IBM hardware to further optimize the automation and standardization of complex server deployments on IBM hardware. Deployment Solution is a ServerProven application and is available directly from IBM.

This IBM Redbook describes the features of Altiris Deployment Solution and explains in detail how to implement features such as managing and deploying firmware updates and hardware configuration changes, image-based and script-based deployments, and integration with the IBM management tools. This book addresses the common issues and recommends best practices to overcome many of the challenges that arise during initial deployment setup.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks